

Lithuania Country Report



About ENISA

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

Contact details

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

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

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



Acknowledgments:

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

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

Legal notice

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

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

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

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

LITHUANIA	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	6
NIS GOVERNANCE	8
OVERVIEW OF THE KEY STAKEHOLDERS	8
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	9
FOSTERING A PROACTIVE NIS COMMUNITY	11
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES	12
SECURITY INCIDENT MANAGEMENT	12
EMERGING NIS RISKS	12
RESILIENCE ASPECTS	13
PRIVACY AND TRUST	14
NIS AWARENESS AT THE COUNTRY LEVEL	15
RELEVANT STATISTICS FOR THE COUNTRY	17
INTERNET ACCESS OF POPULATION AND ENTERPRISES	17
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	18
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	19
OTHER STATISTICS	20
APPENDIX	21
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	21
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	22
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	23
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	23
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	23
REFERENCES	23

Lithuania

The structure of the individual country reports

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

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

National Cyber-Security Strategy

No major changes were noticed in 2010 regarding the national cyber-security strategy. It has been developed but is not yet deployed. A special work group was created by the government in 2010, which designed a general information security strategy. A paper was consequently submitted to the government and the approval and implementation are expected within the two or three coming years. This new strategy will cover the following sectors:

- The public sector (citizens and enterprises);
- The government sector;
- The critical information infrastructure sector.

Action Plan of the Lithuanian Government Programme for 2008-2012

As stated in last year's report, the necessary eGovernment means for the implementation of the eGovernment objectives pointed out in the Lithuanian Government programme¹ are laid down in the Action Plan of the Programme of Lithuanian Government for 2008-2012.

The use of successful and up-to-date telecommunication market liberalisation experience together with encouragement of private initiative and the development of an advanced legal environment for activities will create the necessary preconditions for the adjacent information and communication technologies areas, so that every citizen is able to benefit from ICT, in order to improve his/her living standards and businesses to be able to boost their competitiveness.

Therefore, some of the main eGovernment objectives in the Programme of Lithuanian Government are as follows:

- The development of a Lithuanian Information and Knowledge Society Development Strategy 2009-2015;
- The modernisation of the public administration with regard to the needs of the modern society and the opportunities opened by the ICT;
- The development of eGovernment services bearing in mind the needs of the citizens and businesses;
- The development of a legal framework for the economic regulation of the ICT market and respectively restructure the institutional system by applying common principles to adjacent market segments, i.e. the segments of electronic communication, audiovisual and other content transmitted over electronic networks, electronic signature and information society (eCommerce) services, and by concentrating regulation in the hands of a single competent authority;
- To build a national base for interaction necessary for safe, effective and reliable data exchange among national registers and information systems in Lithuania and across the European Union;
- To use the ICT infrastructure and competencies in the public sector for the more effective functioning of joint service centres;

¹ See: www.epractice.eu/en/document/288296

- To adopt a decision regarding urgently implementing measures and the reinforcement of digital media security and institutional set-up;
- The stimulation of the capacities when using the opportunities provided by the ICT.

Lithuanian Strategy for the Development of the Information Society

As stated in last year's report, the Lithuanian Strategy for the Development of the Information Society² outlines the main aims to be achieved to ensure the development of the information society in Lithuania: the document defines the state's vision, priorities and goals and it also provides the model of implementation and monitoring of this strategy.

It is also worth mentioning that, in February 2010, the Information Society Development Committee under the Government of the Republic of Lithuania approved the **Methodical Requirements for Monitoring of Online Electronic Services**, delivered by State and Local Institutions.

The regulatory framework

Law on Network and Information Security

Lithuania is still waiting for a law on Network and Information Security. A proposal for such a law exists and is in the process of being accepted and implemented.

Law on Legal Protection of Personal Data

The Lithuanian Law on Legal Protection of Personal Data³ was adopted on 11 June 1996 and last amended on 1 January 2009. Its main purpose is the protection of an individual's right to privacy with regard to the processing of personal data. This Law is fully compliant with the EU Data Protection Directive (95/46/EC).

Law on Information Society Services

The Law on Information Society Services was adopted in May 2006. Its aim is to ensure the implementation of EU Directive 2000/31/EC on certain legal aspects of Information Society services and, in particular, electronic commerce in the Internal Market ('eCommerce Directive') by describing and establishing legal grounds for the regulation of the relations to Information Society services.

The law describes Information Society services as services that are normally provided at a distance by electronic means for remuneration and at the individual request of a recipient for such services. It lays down **requirements** for the information provided and the **conclusion of agreements** by electronic means; regulates the responsibility, rights/duties and activities of service providers and, furthermore, establishes the means of dispute resolution.

The law provides that the freedom to provide Information Society services of a subject established outside the Republic of Lithuania may not be restricted, with the exception of established cases related, namely, to intellectual property rights, freedom of choice of law applicable to a contract, among other.

² See: <http://www.epractice.eu/en/document/287686>

³ Source: <http://www.epractice.eu/en/document/288297> . The same source is applicable to other laws and regulations mentioned in this section.

Law on Electronic Communications

Adopted in April 2004 and last amended in March 2009, the Law on electronic communications regulates electronic communications services and networks with their associated facilities and services, the use of electronic communications resources as well as radio and terminal equipment and electromagnetic compatibility. This Law transposes the EU regulatory framework for Electronic Communications. It is currently being improved according to the EU directive on Privacy and Electronic Communications (2002/58).

eIdentity

General overview

Lithuania is replacing its paper national ID card by an eID card since the 1st of January 2009. This national ID card is mandatory and is addressed at Lithuanian citizens over the age of 16. The new eID card complies with the ECC standard⁴.

The authentication certificate contained in both the eID card and the Civil servant eID card is issued through a PKI based system. In the private sector, qualified signature certificates (either soft or on a smart card) also exist. A PKI based system is also available on mobile phones. Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol can be used for validation/management of the certificates' lifecycles.

eSignatures Legislation

Passed on 11 July 2000, the Law on Electronic Signature regulates the creation, verification, and validity of electronic signatures, the rights and obligations of signature users, the requirements for certification services and certification services providers, as well as the rights and functions of the institution of electronic signature supervision.

It is compliant with the EU Directive on a Community framework for electronic signatures (1999/93/EC). The concept of "secure eSignature" stated in the Lithuanian Law is identical to the notion of "advanced eSignature" referred to in the Directive. A secure eSignature created by a secure eSignature-creation-device and based on a qualified certificate which is valid, is granted with the same legal effect as that of a hand-written signature on written documents, also being admissible as evidence before Court.

An amendment to the Lithuanian Law on Electronic Signature was adopted in 2002, which establishes that in all cases, electronic signature shall have the legal power of a hand-written signature, provided that the signature users shall reach an agreement among themselves. In such a way the notion of contractual electronic signature was introduced into Lithuanian law. The law does not mention any specific requirements for the use of electronic signatures in the public sector.

Also worth noting is the fact that Lithuania is a partner in the STORK⁵ (Secure idenTity acrOss borders linKed) project that aims to establish an European eID interoperability platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. The consortium members include national authorities, non profit organisations, private companies and academic partners from: Austria, Belgium, Estonia, Finland, France, Germany, Italy, Lithuania,

⁴ Source: Study on eID Interoperability for PEGS: Update of Country Profiles - <http://ec.europa.eu/idabc/servlets/Docb482.pdf?id=32522>

⁵ The STORK project consortium consists of 29 participants representing 13 Member States and Iceland. A full list of participants in the STORK project is available at www.eidstork.eu

Luxembourg, Netherlands, Portugal, Slovakia, Slovenia, Spain, Sweden, United Kingdom and Iceland.

Law on Identity Cards of the Republic of Lithuania

Adopted in 2001, the Law on Identity Cards⁶ regulates the purpose of the ID card, the procedures for its issuance, change and usage, as well as the data to be engraved. The Law was changed in June 2008 and amended with reference to the fact that the personal identity card shall be used for electronic personal identification and in order to sign electronic data.

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 Transport and Communications • Ministry of Interior, Information Policy Department (MoI) • Police department under the Ministry of Interior of Lithuania • Communications Regulatory Authority of the Republic of Lithuania (RRT) • Information Society Development Committee under the Government of the Republic of Lithuania • State Data Protection Inspectorate • Ministry of Education and Science • State enterprise Infrostruktura under the Ministry of the Interior of the Republic of Lithuania • Ministry of Defence (MoD)
CERTs	<ul style="list-style-type: none"> • CERT-LT • IST-SVDPT • LITNET CERT • Military CERT teams, under the supervision of the Ministry of National Defence
Industry Organisations	<ul style="list-style-type: none"> • Infobalt Lithuania
Academic Organisations	<ul style="list-style-type: none"> • LITNET
Others	<ul style="list-style-type: none"> • ISACA

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁷ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁸.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, eID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

⁶ Source: <http://www.epractice.eu/en/document/288297>

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

⁸ See: <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

As stated in last year's report, there is currently no organization in Lithuania recognized among the NIS stakeholders having the role of a national security agency. Several government bodies, private sector players, and educational institutions, however, are involved with the process.

Co-operation on the development and implementation of national information security policy

As stated in last year's report, the development and the implementation of a national information security policy is being taken care of by the Communications Regulatory Authority of the Republic of Lithuania (RRT) and the Information Policy Department of the Ministry of the Interior (MoI).

The RRT is responsible for private sector supervision while the MoI is charged with setting security policy and coordination of security implementation in governmental sector, information society development policy, development and implementation of eGovernment projects, participation in electronic signature and personal identification projects.

Co-operation via the State Data Protection Inspectorate Personal

The State Data Protection Inspectorate Personal is responsible for data protection in Lithuania. As such, it is responsible for the supervision and the control of enforcement of the Lithuanian law on Legal Protection of Personal Data. The Ministry of Transport and Communications is responsible for implementing and ensuring compliance with the electronic communications legislation in Lithuania. Officially, the ministry is also charged with supervising the transport, post and electronic communications legislation.

CERT-LT was established within RRT to coordinate the existing Lithuanian CERTs and ISPs activities on computer/network/information security.

Co-operation between the CERTs and the Ministry of Defence

The Ministry of Defence operates the incident management centres. However, these are not dealing with network security incidents but instead with physical incidents regarding infrastructure. Lithuania has three Computer Emergency Response Team(s) (CERTs). These are:

- The national CERT-LT, which deals with Internet incidences, improving management systems and procedures, information exchange between CERT and government institutions.
- LITNET CERT, an academic network for dealing with incidents in academia;
- Infostruktura CERT, for public data communication networks. Infostruktura is subordinated to the Ministry of Interior.

As reported in 2010, the CERT system will be re-structured in order to achieve effectiveness gains in the coming years. The open academic CERT LITNET is quite cooperative with the National CERT-LT. They hold meetings and bilateral face-to-face contacts. More working cooperation between the three CERTs is planned for the future. Cooperation with other countries happens via ENISA meetings, where the National CERT-LT is quite active.

The National CERT-LT is also an active member of FIRST. Past incidents are analyzed according to the CERT model. The Ministry of Interior has developed software to compare current with previous incidents. These data points are updated on regular basis.

The CERT-LT's scope of activity is the networks of telecommunication operators and Internet service providers in Lithuania. CERT-LT receives the notifications of telecommunication operators concerning network and information security incidents and threats.

End users should contact their service providers at first. In case the operators can't solve their problems, users can report to CERT-LT. CERT-LT Cooperates with governmental stakeholders such as the State Data Protection Inspectorate and the Cyber-Police and with public institutions such as LITNET, and numerous others groups. CERT-LT interacts with the Ministry of Defence on key security items (escalation of incidents to the MoD if the threat is high).

Co-operation via LITNET, Academic and Research Network in Lithuania

LITNET, Academic and Research Network in Lithuania, is an association of Academic research and other non-profit organizations. The members of this association use, manage, and develop the network.

The highest governing body of LITNET is the LITNET Board whose structure and regulations are under the supervision of the Ministry of Science and Education in Lithuania. The LITNET Board coordinates the development and the management of the network. LITNET gets financial support from the Ministry of Science and Education.

Co-operation via DPA and National Telecom Regulator for the protection of personal data and the fight against spam

The national telecom regulator and the DPA cooperate for the protection of personal data in electronic communications services, including fighting against spam.

Co-operation between ministries, operators and service providers

As stated in 2010, the ministries are not in direct contacts with operators and service providers, the exception being the drafting of legal acts. From the regulator's view point it was stressed that the exchange between providers and authorities regarding the resilience of their networks is not mandatory.

On a quarterly basis, reports are published on the RRT web site dealing with the electronic communications sector. These reports are compiled from information provided by the electronic communication operators and the service providers and aim at providing a good overview of the situation of the communication networks in Lithuania.

They also provide more insights into issues relating to topological and technical matters in network structures as well as security policy issues. Since 2005, these results are made available on the RRT web site⁹.

Resilience issues, limited to incidents, should be better investigated. In this purpose, the RRT is consulting with experts from the EU in a TAIEX project on these matters.

Co-operation between providers and public authorities (public-private partnership)

There are many cases of initiatives between providers and public authorities in Lithuania. However, cooperation between authorities and private organizations is not mandatory for private organisations in Lithuania.

⁹ See: www.rrt.lt/index.php?-447183813

The website www.esaugumas.lt is a good example of Public-Private Partnership (PPP) with the purpose of increasing NIS awareness between the general Internet users, SMEs and Lithuanian governmental institutions.

Since November 2005, a Memorandum on the Progress in the Area of Security of Information and Networks was signed by the Communications Regulatory Authority of the Republic of Lithuania, the Association of Lithuanian Banks and the Association Infobalt. The Parties have agreed to set up a permanent Memorandum Implementation Committee, represented by authorized representatives of the Parties. The Committee shall prepare annual Memorandum Implementation Action Plans and shall take care of implementation of these Plans.

The Lithuanian Ministry of Interior is not directly involved in the fostering of information-exchanges, but cooperation with private sector is one of the ways to implement the strategy the Ministry is pursuing in these matters of improving resilience of state information systems and data communication networks.

Fostering a proactive NIS community

International co-operation via the Cooperative Cyber Defence Centre of Excellence (CCD COE)

Lithuania is actively participating in the Cooperative Cyber Defence Centre of Excellence (CCD COE¹⁰) together with other nations: Estonia, Germany, Italy, Latvia, the Slovak Republic and Spain. CCD COE is located in Estonia and is open to all NATO nations and may cooperate with other nations as contributing participants.

The CCD COE first priorities are to provide insight, subject matter expertise, and assistance to NATO on various aspects of cyber defence: input to concept development, training and exercises, publishing lessons learned, and the development of a legal framework for cyber defence.

¹⁰ See details on the Cooperative Cyber Defence Centre of Excellence at: <http://www.ccdcoe.org/>

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

Security incident management

Since 2006, reports on incidents are made available to the public, on a yearly and quarterly base. A team of specialists from the national CERT-LT team investigates incidents and publishes quarterly reports on those including spam, spyware and malicious software. However, these reports concern only ERC computer response services.

A regulation is in place but there are currently no rules defining the actions to be taken in case an incident happens. There is no clearly specified and institutionalized procedure for incidents reporting. Confidential information that is submitted to the regulator by providers is not made publicly available. Examples for the kind of information this includes are such as:

- Loss of material;
- Loss of money;
- Divulgence of secret information.

On confidentiality issues, Lithuania follows the common CERT model and the way it is used in neighbouring countries: Sweden, Finland, etc.¹¹

Emerging NIS risks

The national risk management process

Lithuania has a few groups working on risk management issues but there is no risk management process in place.

In 2010, a methodology was defined in order to identify all critical nodes and links within the Lithuanian IT infrastructure. The next step will be the implementation of a real-time monitoring of these critical nodes and links, and the production of an online model. Technical decisions remain to be made.

Relevant emerging NIS risks

The Lithuanian national Computer Emergency Response Team (CERT-LT) investigated 10370 security incidents in electronic space during 2010 - about 17 percent less than in 2009 (12539 reports). The requests to investigate the incidents were received from Lithuania's Internet users, Internet service providers and foreign CERT teams.

The problem most frequently faced by the Internet users in 2010 (the same as in 2009) was malicious software – 89.4 percents of all the investigated reports. The majority of incidents were related to the malicious software, which take over the control of the computer and involve it into the botnets network activities.

As in 2009, 2010 saw an increase of incidents related to Web Site Defacement and System Compromise/Intrusion incidents (477 reports) - i. e. two times more than in 2009 (180 reports).

¹¹ Source:

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

Resilience aspects

As stated in last year's report, resilience issues are treated in legislative and regulatory documents on a general level only¹². Common requirements for networks owned or used by public institutions, national regulation requirements regarding the management of information systems and also quality issues have been laid out in a Risk Assessment Manual.

Regulations for security of information systems are in force. However, there is no direct regulation addressing the issue of resilience. The requirements concerning the resilience of network information systems are of secondary implication for private providers. The Department of Electronic Communication Networks within the Communication Ministry targets the private sector. However, as long as there are no attacks, little attention is given to the resilience issue.

The Cabinet of Ministers has just mandated Ministry of Defence to lead a working group (WG) which focuses on issues regarding cyber-security, while the Ministry of Communication renewed the activities of WG with the mandate to address matters of network and information security at legislation level. The important role has WG on national cyber security strategy preparation that is managed by Ministry of Defence. The Ministry of Interior has been kept informed about several initiatives. There are several WGs across ministries addressing information security matters. No documents are yet available on these discussions.

In 2008, RRT started a survey to investigate Lithuanian Internet infrastructure resilience. The main task is to identify critical points of Lithuanian Internet infrastructure and possible risks. In 2007, the Ministry for Interior carried out an audit about security and network operators although it has no direct competence in this area.

Requirements have been developed and implemented for public institutional data communication networks. Here there are plans for establishing and following auditing-type procedures on a regular basis. Also, a security audit regarding data security for state institutions has been undertaken by an external auditor. As far as auditing the measures taken to improve and attain acceptable levels of resilience of public eCommunication networks is concerned, no national regulation defines who has to do this such as specifying the government agency that will do it or if it can be a contractor.

In 2008, the communications Regulatory Authority of the Republic of Lithuania Evaluation performed an evaluation of the Reliability of Lithuania's Internet Infrastructure. During the evaluation of the reliability of interconnection nodes, it became apparent that the terms of connection to Internet Exchange Points (IXP) are not sufficiently transparent in Lithuania; RRT identified that they are not publicly available but that this could help enhance the interconnection between ISPs and thus the reliability of the national Internet infrastructure. RRT also noted that transparency of connection to the IXPs also helps prevent the redirection of national traffic through international ISPs, since IXPs allow direct channels of data transmission traffic to be formed among the Lithuanian ISPs.

This provides an opportunity to reduce costs for international transit services and improves the quality and speed of the Internet connection – factors which are of particular importance to end-users. By evaluating the bandwidth of the international Internet in Lithuania, it was determined

¹² See the ENISA report: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report>

that the total volume of Lithuania's Internet international traffic was about 66.1 Gbps at the end of 2008.

In case of emergency, this bandwidth may be insufficient to cope with a large number of security attacks. Following its investigations into connections to international gateways, RRT concluded that the reliability of international Internet connectivity in Lithuania depends, in effect, on just one international gateway operated by one of the ISPs. Consequently the reliability of Internet operation relies on a single ISP's ability to ensure alternative channels quickly in an emergency and to organise the redirection of data flow, the control of stream priorities, address blocking etc.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Lithuanian Law on Legal Protection of Personal Data dated 11 June 1996 (as modified on 17 July 2000, 22 January 2002 and 21 January 2003) (the "DPA"). The competent national regulatory authority on this matter is the State Data Protection Inspectorate (the "Inspectorate").

Personal Data and Sensitive Personal Data

The definition of personal data in the Lithuanian DPA is based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities and includes any data pertaining to an identifiable individual. There has been no case law or administrative practice challenging the definition and it is being applied increasingly broadly in practice.

Under the DPA, sensitive personal data includes both: (i) the standard types of sensitive personal data; and (ii) information about previous convictions.

Processing of sensitive personal data is generally prohibited. Exceptions are allowed if the standard conditions for processing sensitive personal data are met. Processing of sensitive personal data for medical treatment is allowed when it is in the vital interests of the data subject and he/she is unable to issue consent for such processing due to his/her medical condition. In addition, it is possible to process this data for the prevention and investigation of criminal offences, as well as for litigation purposes.

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

The data controller must comply with the general data security obligations, and shall disclose the particular means applied to the Inspectorate in the notification filings.

Enforcement

The Lithuanian State Data Protection Inspectorate has no power to impose penalties for violations of the DPA, although it is entitled to take enforcement action including carrying out investigations and issuing mandatory orders. Prosecutions for violations of the DPA are brought before the Lithuanian general practice courts and are heard by one judge, who may impose penalties. Decisions of the court may be appealed to the High Administrative Court of the Republic of Lithuania.

NIS awareness at the country level

Awareness actions targeting the consumers/citizens

The project "Safer Internet LT"¹³ is designed to promote safer use of the Internet and new online technologies for children and youth, to help children, parents and educators to avoid the dangers associated with the illegal and harmful content on the Internet, especially raising awareness of the parents. The project is also committed to run a hotline for internet users in Lithuania. This project is a successor of the projects "Safer Digital Lithuania" and "Hotline Lithuania" carried out in the period 2005 - 2007. The contract has been renewed until 2012.

"Safer Internet LT" is made up of a consortium of two partners who have extensive experience working together.

Communications Regulatory Authority of the Republic of Lithuania (Coordinator of consortium) is national regulator which responsibilities among others are the work on the consumer education and awareness raising, reduction of negative impact of network and information security incidents and illegal content, management of network and information security incidents (CERT functions), encouragement of the development of legal and standardisation measures of network and information security.

Ministry of Education and Sciences of the Republic of Lithuania is committed to prevention of harmful content. It is the best multiplier in the country with its network of education centres (schools, universities, etc.) and is a good relay to disseminate information about internet safety and hotline actions.

Objectives:

- Act as node of awareness network in Lithuania. Devise a cohesive, hard-hitting and targeted awareness campaign using the most appropriate media, taking into account best practice and experience in other countries;
- Establish and maintain a partnership (formal or informal) with key players (government agencies, press and media groups, ISP associations) and actions in their country relating to safer use of Internet and new media;
- Co-operate with work in the wider field of media and information literacy;
- Inform users about European filtering software and services and about hotlines;
- Actively co-operate with other national nodes in the European network by exchanging information about best practices, participating in meetings and designing and implementing a European approach, adapted as necessary for national linguistic and cultural preferences;
- Provide a pool of expertise and technical assistance to start-up awareness nodes (new nodes could be 'adopted' by a more experienced node).

Awareness actions targeting the industry

The Lit-Grid Program is a long-term program (2007-2012) and is a government-financed process aimed at deploying, developing, and supporting Lithuania's grid computing, service, and communications infrastructure for the purposes of research and education. The grid is to be integrated into the emerging European and Baltic grid infrastructures, and knowledge about grid technologies and the use of grids in Lithuania is to be brought up to the level which exists in those EU member states that have a longer history of experience with such issues.

¹³ See: http://ec.europa.eu/information_society/activities/sip/index_en.htm

Furthermore, Lithuania is expected to do more work in defining grid technology policies and in setting standards in this process. The Lit-Grid Program is working on grid-based, parallel and distributed algorithms and other high-performance computing procedures for various research applications that are of interest and importance to Lithuanian scientists.

Infobalt represents its members in state authorities and management institutions, stimulates cooperation and common activities preparing and implementing national development strategy for ICT sector. Simultaneously the association emphasizes the importance of cooperation among high education, scientific research and ICT sector and initiates activities of such cooperation.

By stimulating exchange of experience, introduction of innovations and more active involvement of society into knowledge society creation processes, the association has already organized fourteen annual exhibitions "Infobalt"¹⁴ and nine international conferences devoted for discussions related to innovation processes.

Seeking amplification of competitiveness of national companies and Lithuanian market in EU and the whole world, the association intensively works in the field of international cooperation. "Infobalt" has become a member of international structures in ICT industry EICTA and WITSA, exchanges knowledge with representatives of national ICT sectors of European and other countries.

Activities of "Infobalt" are actively supported by the Government of the Republic of Lithuania and responsible institutions, and Prime Minister of the Republic of Lithuania pays personal attention to annual events.

Awareness measures to combat spam and/or malware

The websites of the telecom regulator (on behalf of the national CERT) and the DPA provide specific information on spam, spyware, malicious software and actions to prevent them. Lithuania can be considered as a Member State with little information on the actions and measures related to the combat against online malpractices.

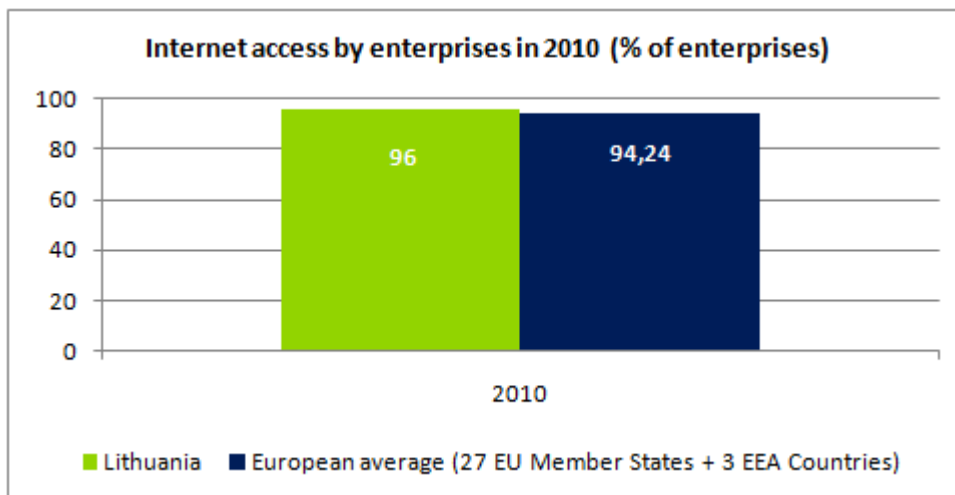
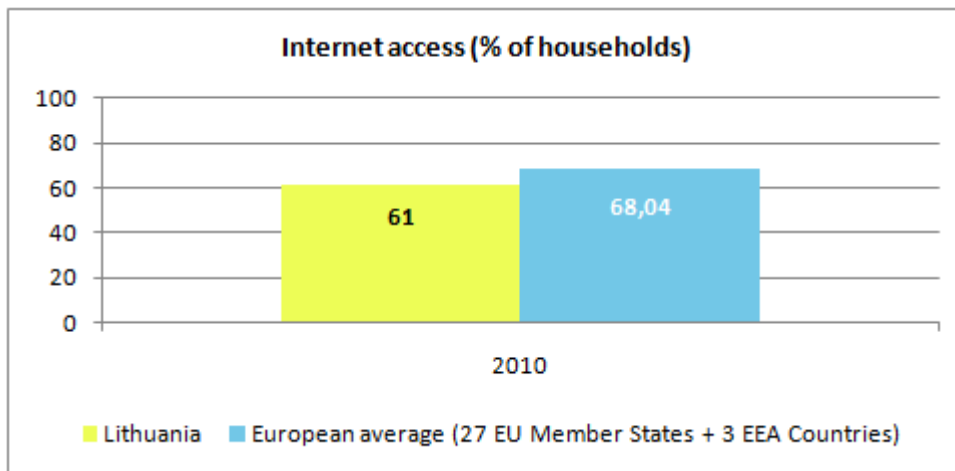
¹⁴ See: www.infobalt.lt/sl/index_lt.html

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Lithuania, a series of relevant statistics are included in this section. Some of them indicate that the information society in Lithuania is at a relatively early stage of development, while others show progress and interesting trends.

Internet access of population and enterprises

The following graphs provide an overview of the situation¹⁵ of Internet access in Lithuania for enterprises and respectively households, relative to the European average.

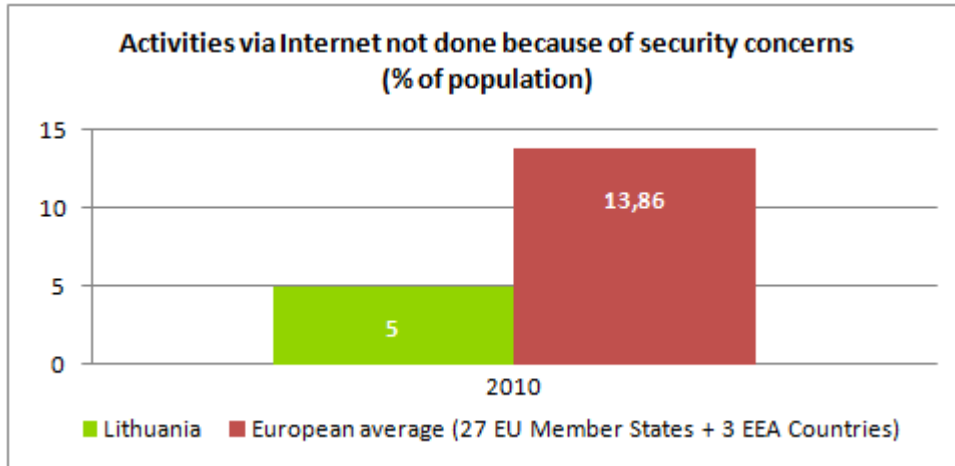


In 2010, the statistics indicate that the enterprises in Lithuania a level of Internet access that is slightly above the European average, while more effort is required to close the gap on the households.

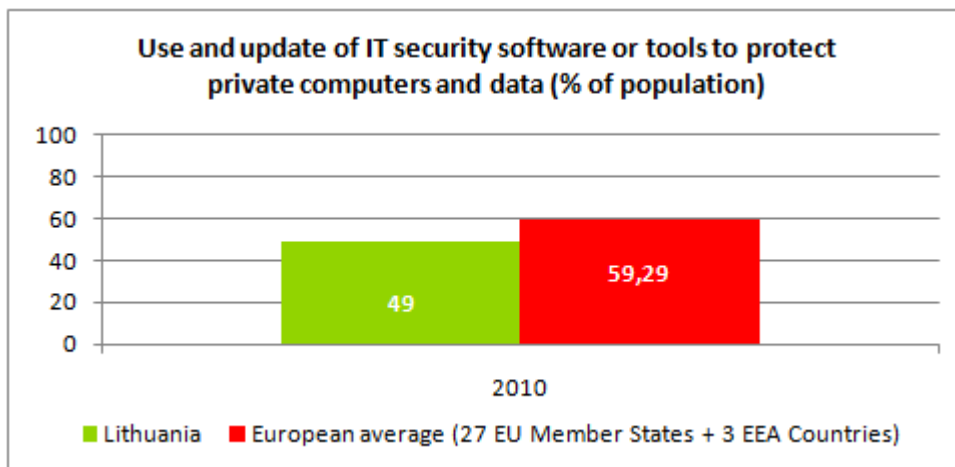
¹⁵ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Lithuania 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 a third of the European average:



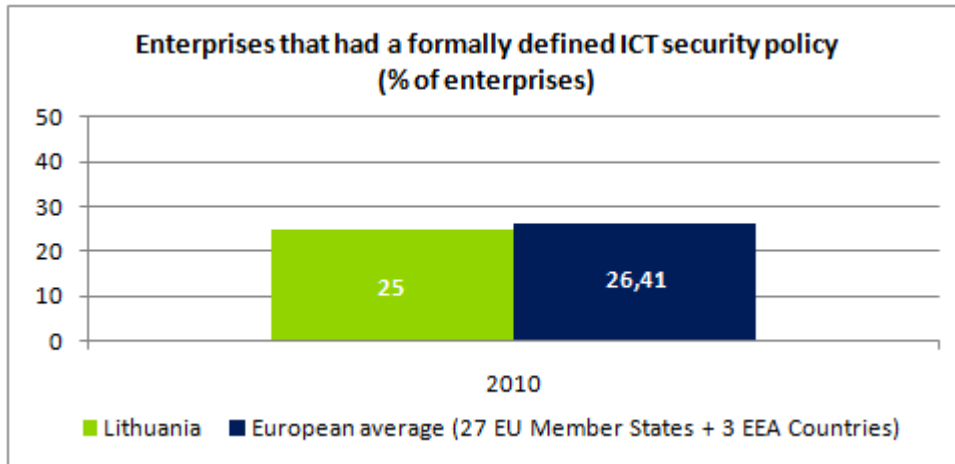
This can be either an indication of much confidence in web-based transactions or an indication of less awareness of the general public regarding IT threats.



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

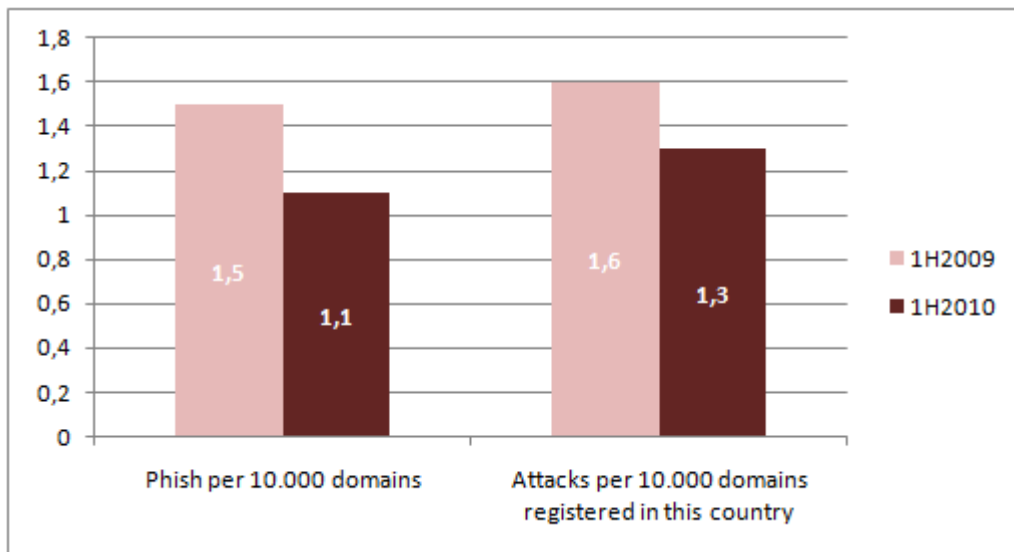
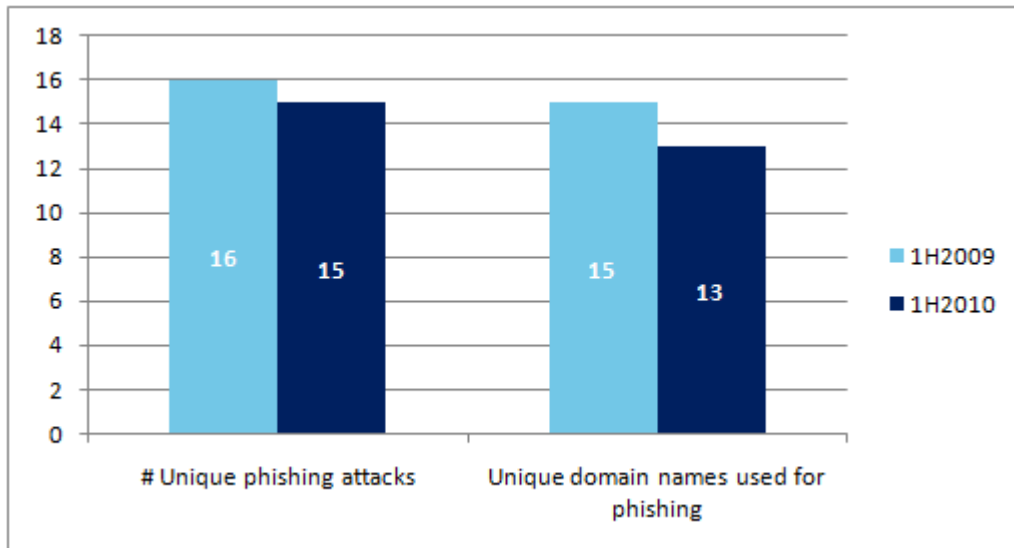
Statistics on use of Internet by enterprises and related security aspects

The percentage of enterprises in Lithuania that have a formally defined ICT security policy is at about the same level as their European peers' is. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Malta was mentioned in the global report¹⁶ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁶ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Transport and Communications	The Ministry of Transport and Communications is in is responsible for the development and implementation of Security Technology and Standards Policy.	www.transp.lt
2. Ministry of the Interior, Information Policy Department (MoI)	Ministry of the Interior, Information Policy Department, is responsible for the development and implementation of Security Technology and Standards Policy.	www.vrm.lt
3. Police department under the Ministry of the Interior of Lithuania	Police department under the Ministry of the Interior of Lithuania is responsible for safeguarding national legislations.	www.cyberpolice.lt
4. Communications Regulatory Authority of the Republic of Lithuania (RRT)	The Communications Regulatory Authority of the Republic of Lithuania (RRT) is an independent national institution regulating communications sector in Lithuania. RRT mission is to ensure a variety of technologically progressive, top quality, safe and affordable information and communications technologies (ICT) and postal services/products to every citizen of Lithuania as well as to create favourable conditions for ICT and postal business development, in this way promoting information and knowledge society progress.	www.rrt.lt
5. Information Society Development Committee under the Government of the Republic of Lithuania	Information Society Development Committee under the Government of the Republic of Lithuania is responsible to design, arrange and co-ordinate processes aimed at the development of information society alongside the creation of an open, educated, continuously learning society, members of which rely on knowledge in their activities, have an opportunity and capability to make effective use of modern ITT means in every step of their life.	www.ivpk.lt
6. State Data Protection Inspectorate	The State Data Protection Inspectorate is responsible for the supervision and control of enforcement of the Republic of Lithuania law on Legal Protection of Personal Data.	www.ada.lt
7. Ministry of Education and Science	The Ministry of Education and Science formulates and executes the national policy in the areas of education, science and studies, drafts strategic education plans, annual programmes, submits proposals and resolutions to the Government, organises mature examinations, approves the general content of teaching, training and studies under the framework of formal education, national standards for attained education levels, standards for vocational training, guidelines for study areas in higher education, accreditation criteria applicable to curricula and the order of accreditation. Included in this would be curriculum for IT and security courses included within.	www.smm.lt
8. State enterprise Infostruktura under the Ministry of the Interior of the Republic of Lithuania	State Enterprise „Infostruktura" is administrator of the Secure State Data Communication Network (SSDCN), which is isolated from the Internet and provides the secure national-wide communication services for public institutions in Lithuania, also provides communications via SSDCN and TESTA with the National Networks of EU Member States, EU Institutions and EU Agencies. TESTA is the	www.is.lt www.svdpt.gov.lt

National authorities	Role and responsibilities	Website
	European Community's own private network, also isolated from the Internet and allows officials from different Ministries and administrations to communicate at a trans-European level in a safe and prompt way.	

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST¹⁷ member TI¹⁸ listed 	
9. CERT-LT	CERT-LT is the National cert of Lithuania. The main purpose of the team is to handle security problems such as computer security incidents. Fields of operation: computer security incident response: investigation, coordination, consulting, incident detection, prevention. CERT-LT is FIRST member and TI listed.	www.cert.lt
10. IST-SVDPT	IST-SVDPT is the Secure State Data Communication Network CERT of Lithuania. State Enterprise „Infostruktura" is administrator of the Secure State Data Communication Network (SSDCN), which is isolated from the Internet and provides the secure national-wide communication services for public institutions in Lithuania, also provides communications via SSDCN and TESTA with the National Networks of EU Member States, EU Institutions and EU Agencies. TESTA is the European Community's own private network, also isolated from the Internet and allows officials from different Ministries and administrations to communicate at a trans-European level in a safe and prompt way. The SSDCN is delivering this type of services: Secure encrypted data communication between Governmental institutions of the Republic of Lithuania; Connection to the IDADBC program networks for Interchange of Data between administrations in EU; Secure communication with non-administrative organizations and citizens; Electronic mail relay for closed user groups; Secure hosting of workstations and information data bases; Delivery of classified information to authorized users in Lithuania and in EU. IST-SVDPT is FIRST member and TI listed.	www.svdpt.gov.lt
11. LITNET CERT	LITNET-CERT is the CERT of LITNET - Academic and Research Network in Lithuania. CERT-LT is the Lithuanian 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. LITNET CERT is FIRST member and TI listed.	http://cert.litnet.it
12. Military CERT teams	The Ministry of Defence disposes of four military CERT teams that are in close relationship with the national CERT team, CERT-LT.	No website available

¹⁷ See: <http://www.first.org/members/teams/>

¹⁸ See: <http://www.trusted-introducer.nl/>

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
13. Infobalt Lithuania	Infobalt's goal is to help promising IT companies to penetrate into world markets. Association "Infobalt" unifies Lithuanian IT, communications and electronics companies, as well as scientific institutions, seeking to represent national ICT sector. The association participates in solving strategic sector's development questions and influences the development itself.	www.infobalt.lt

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
14. LITNET	LITNET is an association of Academic research and other non-profit organizations. The members of this association use manage and develop the network.	www.litnet.lt

Other bodies and organisations active in network and information security

Academic Organisations	Role and responsibilities	Website
15. ISACA	ISACA is a worldwide association of IS professionals dedicated to the audit, control and security of information systems. The Lithuanian chapter organizes local events such as education and training, workshops and other specific events.	www.isaca.lt

References

- An overview of the eGovernment and eInclusion situation in Europe, available at www.epractice.eu/en/factsheets
- See the information on: www.esauqumas.lt with regards to the public-private partnership in Lithuania for increasing of NIS awareness between SMEs, general users and public authorities.
- ENISA, "Information security awareness in financial organization", November 2008, available at: www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- ENISA report "Analysis of Member States policies and regulations - Policy Recommendations" available at: www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations

