

# Latvia Country Report



## About ENISA

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

## Contact details

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

### Mr. Giorgos Dimitriou

ENISA External Relations Expert

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

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



## Acknowledgments:

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

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

<b>LATVIA.....</b>	<b>4</b>
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS .....	4
<b>NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES.....</b>	<b>5</b>
OVERVIEW OF THE NIS NATIONAL STRATEGY .....	5
THE REGULATORY FRAMEWORK .....	5
<b>NIS GOVERNANCE .....</b>	<b>8</b>
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 .....	10
<b>COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....</b>	<b>11</b>
SECURITY INCIDENT MANAGEMENT .....	11
EMERGING NIS RISKS .....	11
RESILIENCE ASPECTS .....	11
PRIVACY AND TRUST .....	12
NIS AWARENESS AT THE COUNTRY LEVEL .....	13
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY .....	14
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION 14	
<b>RELEVANT STATISTICS FOR THE COUNTRY .....</b>	<b>15</b>
INTERNET ACCESS OF POPULATION AND ENTERPRISES .....	15
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS.....	16
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS .....	17
OTHER STATISTICS .....	18
<b>APPENDIX.....</b>	<b>19</b>
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY .....	19
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs) .....	21
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	22
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES .....	24
REFERENCES .....	24

## Latvia

### 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

Significant changes have been launched in 2010 regarding NIS national strategy in Latvia, the main one being the **National Security Concept** which has been approved by the Cabinet of Ministers but yet has to be confirmed by the Parliament. This document determines the basic strategy principles, priorities and measures for the prevention of danger to the State. It is defined for a period of four years.

A section of this document is dedicated to Information Technology risk prevention, and defines how to provide IT security and how to improve the existing mechanisms. Currently, Latvia assesses its enterprises as being under a moderate risk and that there is no significant impact existing towards national security. However, it is expected that, in the near future, electronic attacks will increase in numbers and methods. This brings the possibility that some attacks may paralyze certain IT related activities. Therefore, Latvia defined priorities regarding cyber threats by improving the legal framework, as well as inter-institutional and international co-operations.

### The regulatory framework

#### Information Technologies Security Law

This new law, adopted by the *Saeima* (Parliament) on 28 October 2010 – came into force on 1 February 2011, aims to improve information technologies security by defining the key requirements for organizations to guarantee the security for the essential electronic services.

The Law's intended activities are the following:

- Identification and protection of critical infrastructure;
- Establishment of IT Security Incident Response Institution (national CERT), including provision of its tasks and rights: organization of the training measures, provision of effective support to the national police forces, enablement of effective interactions with foreign partners;
- Determination of the behaviours in the cases of information technology security incidents;
- Setting-up minimum security requirements of state and municipal institutions (currently the statutory safety requirements in fact applies only to state information systems and classified information processing systems);
- Responsibilities of electronic communications service providers for the implementation of the Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services.

It also foresees that the state, the municipal institutions and the private sector legal entities are obliged to cooperate with the IT Security Incident Response Institution in carrying out its legitimate requirements.

### **State Information Systems Law**

The State Information Systems Law provides a legal framework for the operation of state information systems and the cooperation of involved organisational units. Adopted in May 2002, with amendments until 2008 this law is aimed at ensuring the availability and quality of the informative services provided by state and local government institutions in the state information systems.

Information Systems Law foresees Operating Principles for State Information Systems:

- The State Information Systems shall be merged within an integrated state information system. It is prohibited to collect data subjects and enter data into the state information system databases which are accessible in the integrated State Information System;
- During the course of operation of State Information Systems, regarding the data subject and their cognizable objects information shall be registered only once. The identification of objects should be prescribed by regulatory enactments, ensuring the updating of data.
- The State Information Systems Law also provides rules for security of state information systems.

### **Personal Data Protection Law**

The Law on Personal Data Protection was adopted by the Latvian Parliament on 23 March 2000 and was lastly amended by Law of 19 December 2006. It is based on standard fair information practices and is fully compliant with the EU Data Protection Directive (95/46/EC).

The aim of this Law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, with respect to the processing of personal data. Application of the Law is overseen by the State Data Inspectorate.

### **Electronic Communications Law**

The Electronic Communications Law was adopted on 28 October 2004 and entered into force on 1 December 2004. It aims to promote and regulate the provision of electronic communications services, transposing the EU regulatory framework for electronic communications. The law provides for forms of various electronic networks, including both public and private electronic networks. It also provides for duties and rights of providers, subscribers, and users of electronic networks.

Communication service providers must take appropriate technical and organisational measures regarding security of its services and users' data protection. In case of particular security threat providers should inform users on the risks and available means of protection to minimize the risks.

### **Sections of the Penal Code referring to IT Security**

Several sections of the Latvian criminal law are related to cyber crime and security, like for instance:

- Section 241. "Arbitrarily Accessing Automated Data Processing Systems";
- Section 243. "Interference in the Operation of Automated Data Processing Systems and Unlawful Actions with the Information included in Such Systems";
- Section 244. "Unlawful Operations with Automated Data Processing System Resource Influencing Devices";
- Section 245. "Violation of Safety Provisions Regarding Information Systems".

## Self-regulations

*Self-regulatory Code of Conduct for the Protection of Children in the Field of Mobile Communications in Latvia.*

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

## eIdentity

*General overview*

Latvia recently started issuing electronic identification cards for its citizens over the age of 15.

In Latvia, electronic authentication through private sector smart cards is based on PKI systems. The certificates used are issued by the State Revenue Services and require a passport to be requested. The methods used for the validation of certificates and/or the management of their lifecycles include Certificate Revocation Lists (CRLs, and delta CRLs) and the Online Certificate Status Protocol (OCSP).

Non-PKI based systems are also in place, based on either multifactor or single factor authentication.

*Electronic Documents Law*

The Electronic Documents Law was adopted by the Latvian Parliament on 31 October 2002 and came into force on 1 January 2003. It transposes the EU Directive on a Community framework for electronic signatures (1999/93/EC) and defines the legal status of electronic documents and digital signatures.

The Law sets an obligation for state and local government institutions to accept electronic documents from natural persons and legal persons no later than 1 January 2004. Due the introduction of a qualified e-Signature in September 2006 by the Latvian Post, all state and municipal authorities have to accept documents signed with such a qualified electronic signature.

## NIS Governance

### Overview of the key stakeholders

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

<b>National Authorities</b>	<ul style="list-style-type: none"> <li>• Ministry of Transport (and Communications)</li> <li>• IT Security Incident Response Institution (CERT.LV)</li> <li>• National IT Security Council</li> <li>• Data State Inspectorate</li> <li>• Ministry of Environmental Protection and Regional Development</li> <li>• State Police</li> <li>• Ministry of Education and Science</li> <li>• Ministry of Defence</li> <li>• Ministry of Interior</li> </ul>
<b>CERTs</b>	<ul style="list-style-type: none"> <li>• CERT.LV<sup>1</sup></li> </ul>
<b>Industry Organisations</b>	<ul style="list-style-type: none"> <li>• Latvian Information and Communication Technology Association (LIKTA)</li> <li>• Internet Association of Latvia (LIA)</li> <li>• Information Systems Audit and Control Association (ISACA) Latvia</li> <li>• Telecommunication Association of Latvia (LTA)</li> <li>• Association of Computer Technologies of Latvia (LDTA)</li> <li>• Latvian Electrical Engineering and Electronics Industry Association (LEtERA)</li> </ul>
<b>Academic Organisations</b>	<ul style="list-style-type: none"> <li>• University of Latvia, Institute of Mathematics and Computer Science</li> <li>• Riga Technical University</li> <li>• Institute of Electronics and Computer Science</li> </ul>

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"<sup>2</sup> – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory<sup>3</sup>.

**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.

<sup>1</sup> As of 01 February 2011, the two previous CERT teams (DDIRV and CERT NIC.LV) have merged into one national CERT team.

<sup>2</sup> The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

<sup>3</sup> Source: <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 via the Ministry of Transport**

The Ministry of Transport is the main ministry in terms of IT security matters. It is responsible for the development of policies, supervises the IT Security Incident Response Institution (CERT.LV) and leads the National IT Security Council.

### **Co-operation via the Ministry of Environmental Protection and Regional Development**

The Ministry of Environmental Protection and Regional Development is responsible for both the development and the implementation of information security policies at the national level. The ministry organizes and coordinates the development and the implementation of the state policy in the field of electronic government, information society and IT and also facilitates and coordinates the development of state and local governments' electronic services.

### **Co-operation via the National IT Security Council**

The National IT Security Council stands as a coordination mechanism. It replaces the previous Consultative Council of Security for Electronic Communications & Information Technologies.

### **Co-operation with the Data State Inspectorate**

The Data State Inspectorate is a state authority that is responsible for the control and the supervision of the state-wide processing of personal data in compliance with the requirements of the Personal Data Protection Law. The Data State Inspectorate is under the supervision of the Ministry of Justice.

### **Co-operation via the LV CSIRT initiative**

LV CSIRT is a forum of computer incident response teams and security specialists from various organizations in Latvia. Several workshops and meetings are organized to discuss issues of common interest.

The main goals of the forum are to exchange contact information, to collaborate on incident response and to exchange experience on different computer security related topics. As a forum it does not handle incidents but fosters closer collaboration and better communication amongst public and private organizations in Latvia.

### **Other co-operation of NIS stakeholders against spam and malware**

There is a co-operation against spam and malware between different national bodies. The national DPA, the consumer rights protection centre and the public utilities commission cooperate for the protection of personal data in electronic communications services, including the fight against spam. Also, at an international level, Latvia participates in the CNSA (Computer Network Security Awareness) and the LAP (London Action Plan).

Latvia's spam blacklist (MMS – see <http://blw.cert.lv>) has been created with the intention of blocking the IP addresses of spammers. It is a project initiated by INBOX.LV and CERT NIC.LV and supported by LV CSIRT.

Latvia's spam-blocking helps to reduce the number of spam mail sent and received in Latvia, lessen the risk that Latvian IP addresses will be included in foreign blacklists, strategically respond

to local *botnet* flare-ups, assist users in recognizing hacking or viruses and relieve communications channels between Latvia and the rest of the world.

Latvia's MMS is created either manually – IP addresses are added to the list by service providers associated with the project or automatically – e-mail service providers filter spam letters.

### **Fostering a proactive NIS community**

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

As stated in last year's report, Latvia is participating in the Cooperative Cyber Defence Centre of Excellence (CCD COE) together with other sponsoring nations: Estonia, Germany, Italy, Hungary, Lithuania, 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.

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

### Security incident management

Latvia has an independent public utility regulator: the Latvian Public Utilities Commission (PUC). It supervises communication service providers and network operators as far as tariffs and access are concerned.

End-users can submit spam complaints to the consumer protection centre and the national DPA. The site netsafe.lv is partially state funded and aims at increasing the safety of children on the internet. It also allows for the possibility to lodge complaints but is not specifically dedicated to spam.

### Emerging NIS risks

#### The national risk management process

Since the beginning of 2010, things started to move efficiently in terms of national risk management. This brought major changes to the national risk management process that was almost not existent. Predominately, new laws have been drafted and applied in order to clearly define how risks are identified and how incidents are managed (see above, in section "Regulatory framework").

#### Relevant emerging NIS risks

As in most countries around the world, Latvia faces increasing numbers of botnets, malware distribution and spam e-mail.

### Resilience aspects

Compared with 2010, the Ministry of Transport is still the only one responsible for issues related to resilience and the policy development.

The primary regulations regarding resilience of the public eCommunications networks in Latvia are laid down in the IT Security Law that defines the overall roles and responsibilities towards continuity aspects.

As far as known in Latvia there is not yet available a centralised repository of resilience good practices and there are no specific initiatives between providers and public authorities regarding resilience aspects.

## Privacy and trust

### Status of implementation of the Data Protection Directive

The Latvian Law <sup>4</sup>on Personal Data Protection (the "Data Protection Act" or "DPA") was adopted by the Latvian Parliament on 23<sup>rd</sup> of March 2000 and was lastly amended on 1 July 2009. It incorporates the principles and provisions of the Data Protection Directive. The competent Latvian national regulatory authority on this matter is the State Data Inspection (the "SDI").

### Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is closely based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities. Under the Latvian DPA, sensitive personal data means the standard types of sensitive personal data. There is a general ban for the processing of sensitive personal data. As an exception, sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met or one of the alternative grounds set out in Latvian law are satisfied. Any consent for the processing of sensitive personal data must be in writing.

These alternative grounds are processing: (i) carried out for non-commercial purposes by private entities provide the data only relates to members of that entity and are not disclosed to third parties; (ii) necessary for providing social aid; (iii) to develop the Latvian national archives; (iv) necessary for statistical surveys performed by the Central Statistical Bureau; (v) necessary for administrative functions or developing the state information systems; or (iv) necessary under an insurance contract.

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

The data controller and the data processor must comply with the general data security obligations. The mandatory technical and organisational requirements for protection of personal data processing systems are established by the Cabinet of Ministers of the Republic of Latvia in the form of specific regulations.

### Data protection breaches

The DPA requires the data controller to notify third parties if they receive incorrect or illegal personal data. Any person that holds personal data without legal grounds shall delete the data right away. The DPA, however, does not oblige the data controller to notify the data subject about illegalities discovered in processing.

### Enforcement

Complaints concerning violations in the field of personal data protection are reviewed by the SDI, which is also authorised to impose penalties. A report on the alleged violation of personal data protection is prepared by the inspector of the SDI or other SDI employee who initiates examination of the case. Following the completion of the examination of the case, the director of the SDI or the administrative punitive commission of the SDI makes a decision imposing either penalties or sanctions.

---

<sup>4</sup> See also the Publication: "eGovernment in Latvia" available at <http://www.epractice.eu/>

The type of penalty or sanction depends on the severity of the violation and can either be a warning, fine or prohibition on data processing. The breaches of the DPA result in administrative liability in accordance with the Code of Administrative Offences of Latvia.

## **NIS awareness at the country level**

### **Awareness actions targeting the industry**

The Latvian Internet Association (LIA) is a public organisation of national Internet service providers acting for the development of the Latvian internet landscape. The participation of LIA clearly demonstrates the will of Latvian ISPs to enhance internet services in Latvia. The main role of LIA within the project will be to ensure efficient communication with Latvian ISPs as well as to involve various experts from the IT industry.

If clients request then ISPs should provide their clients information on possible vulnerabilities and risks and provide (web-based) spam filters, use blacklists, etc. Banks inform and warn clients via their website about the risks of internet banking, in particular phishing, of which many clients had become victim.

### **Awareness actions targeting the consumers/citizens**

As stated in last year's report, the Net-Safe Latvia<sup>5</sup> project became an awareness centre combining awareness work, hotline and helpline in January 2009. As an awareness centre the project is implemented by The State Regional Development Agency, Latvian Internet Association and the State Children Rights Inspectorate.

The aim of the awareness centre is while informing about the possibilities provided by internet, warn about the potential threats and to provide facilities which can help to deal with illegal internet content and braches online. Three main target groups have been indicated by the project – children, their parents/caretakers, teachers/educators.

Net-Safe Latvia project is the recognized in society as a valuable and needed project dealing with internet safety issues. Project has strong support from national stakeholders including Law Enforcement, Industry, educational institutions and several NGO's.

The centre initiates, coordinates and participates in a broad range of activities and initiatives, promoting safer use of internet for all indicated target groups. Among others:

- National campaigns;
- Educational Seminars;
- Youth Panel;
- Development of educational materials;
- Research.

**The Latvian Safer Internet Centre<sup>6</sup>** – Net-Safe Latvia project – has a combined web page containing all information on the work of the awareness centre, hotline and helpline; it is available in Latvian, Russian and English: <http://www.drossinternets.lv>

<sup>5</sup> Source: [http://www.canee.net/net\\_safe\\_project\\_in\\_latvia](http://www.canee.net/net_safe_project_in_latvia)

<sup>6</sup> Source: [http://www.saferinternet.org/web/quest/centre/-/centre/latvia?p\\_p\\_lifecycle=1&p\\_r\\_p\\_1607082367\\_country=Latvia&](http://www.saferinternet.org/web/quest/centre/-/centre/latvia?p_p_lifecycle=1&p_r_p_1607082367_country=Latvia&)

The coordinators of the Latvian Awareness Centre:

- State Regional Development Agency;
- Latvian Internet Association;
- The State Inspectorate for Protection of Children Rights.

Also, CERT NIC.LV has developed educational posters for children and adults, explaining how one should behave online and what are the threats.

Additionally, CERT.LV together with the LV-CSIRT initiative group has started the development of an IT security education portal, [www.esidross.lv](http://www.esidross.lv) ("Be Safe"). This portal will provide information on how to keep one's computer safe, how to shop on-line safely, etc. The materials contained in this portal will be in Latvian and targeted to non-IT professionals.

CERT.LV will also launch a series of educational seminars in 2011, in order to increase the level of awareness and education among representatives of state and municipal organisations as well as from the private sector.

### **Regional Awareness**

The regional "Baltic IT&T 2010 Forum: eBaltics" took place in April 2010 in Riga. This is one of the most significant ICT events in the Baltic Sea Region, bringing together senior government representatives, experts from European Commission and international organisations, as well as top level executives from the world's leading ICT companies and other business sectors.

The 2010 forum addressed a series of relevant network and information security topics like for example:

- IT security trends;
- Secure Information Technology for the Society;
- Network and information security challenges today;
- Internet Resilience.

Some of the recognised benefits of the forum are related to the opportunities for exchange of good practice and cooperation between representatives of ICT industry, CIOs, business executives, public sector and representatives from other fields; co-operation in cross-border projects in the Baltic Sea Region and Central and Eastern European Countries; development of expert and organizational networks.

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

As stated above, CERT NIC.LV, CERT.LV and LV-CSIRT participated in initiatives providing information on secure use of IT resources to the general public as well as representatives of state and municipal organisations and from the private sector.

### **Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection**

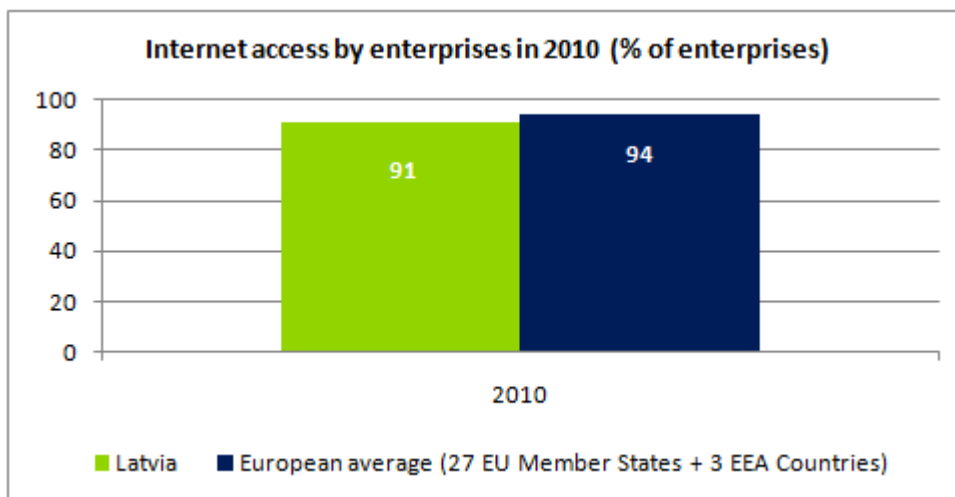
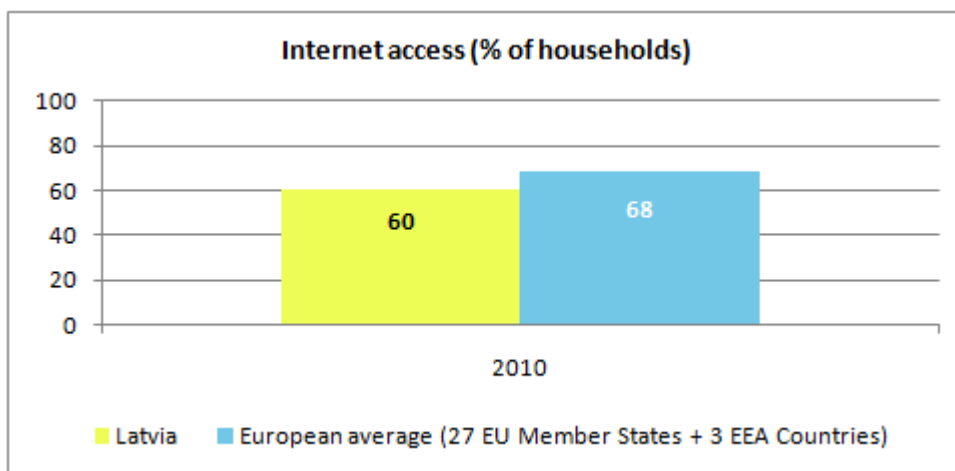
The IT Security Law that enters in effect February 2011 features a set of measures aiming at improving Critical Information Infrastructure Protection.

## Relevant statistics for the country

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

### Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation<sup>7</sup> of Internet access in Latvia for enterprises and respectively households, relative to the European average.

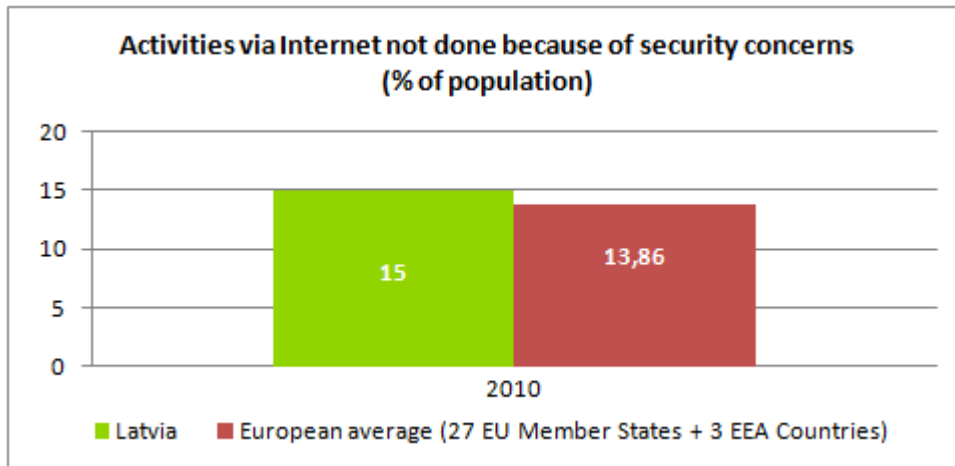


In 2010, the statistics indicate that the enterprises in Latvia have almost the same level of Internet access as the European average, while more effort is required to close the gap on the households.

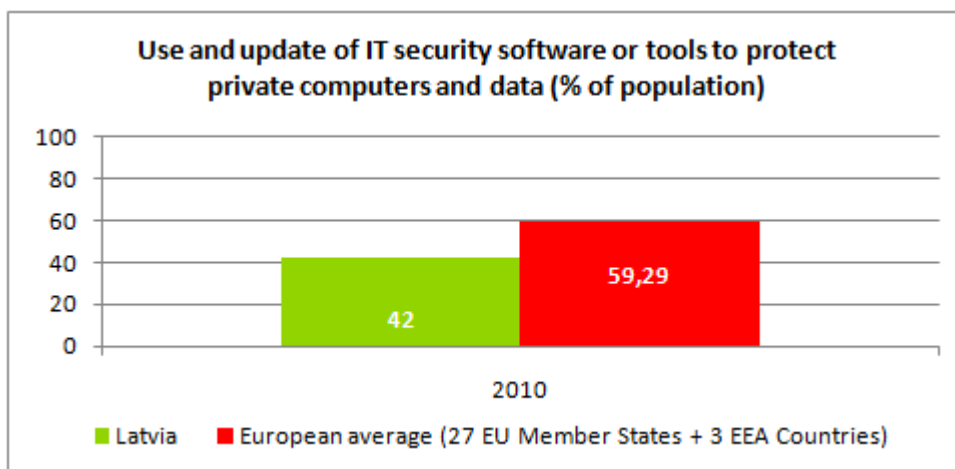
<sup>7</sup> Source: Eurostat

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

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



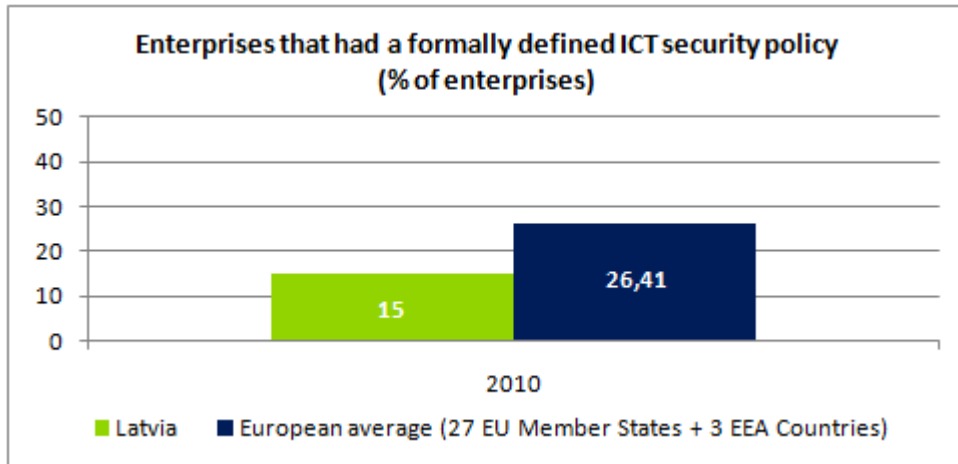
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



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

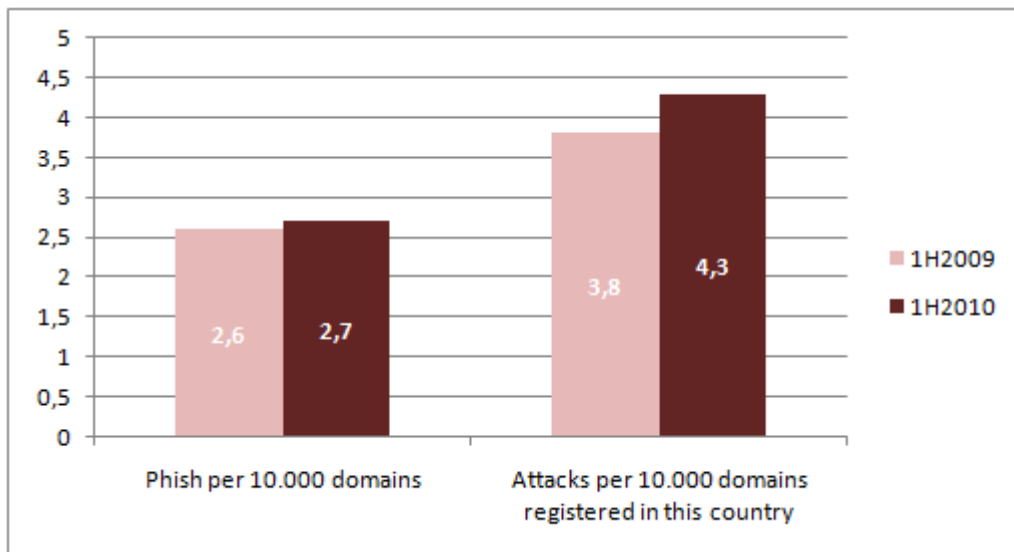
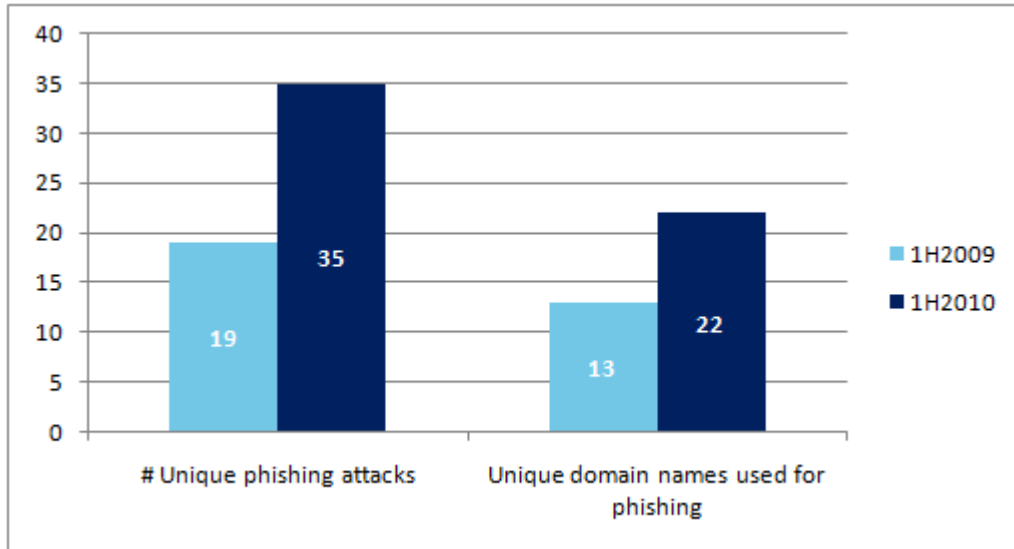
## Statistics on use of Internet by enterprises and related security aspects

Fewer enterprises in Latvia have a formally defined ICT security policy, compared with their European peers. See below:



## Other Statistics

It is interesting to also mention that during the 1<sup>st</sup> half of 2010, and respectively for the 1<sup>st</sup> half of 2009, Latvia was mentioned in the global report<sup>8</sup> published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



<sup>8</sup> See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_1H2010.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf)

## APPENDIX

### National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of Transport (and Communication)	<p>The Ministry of Transport is the main ministry in terms of IT security matters in Latvia. Its responsibilities are the elaboration of the transport, communication policy, organization and coordination of the implementation of transport, communication policy, as well the execution of other functions as laid out in normative acts. The main tasks of the Ministry of Transport are:</p> <ul style="list-style-type: none"> <li>To elaborate state policy in transport and communications sectors (documents of policy planning) and coordinate its implementation;</li> <li>To provide the attraction of financial resources to implement the state policy in transport and communication sectors;</li> <li>To participate in elaboration of EU legal acts, identifying and defending Latvian interests;</li> <li>To elaborate legal acts regulating the transport and communication sectors;</li> <li>And within the competence of the Ministry to provide their implementation and control.</li> </ul>	<a href="http://www.sam.gov.lv">www.sam.gov.lv</a>
2. National IT Security Council	<p>This authority was previously known as the Consultative Council of Security for Electronic Communications and Information Technology. It is chaired by a representative from the Ministry of Transport and consists of representatives from all state institutions involved in the security of electronic communications and information technology. Its function is to coordinate planning and implementation of tasks and arrangements related to information technologies security.</p>	No website available
3. Data State Inspectorate	<p>Control and supervision of processing of personal data state-wide in compliance with requirements of the Latvian Personal Data Protection Law. The main task of the Data State Inspectorate are to:</p> <ul style="list-style-type: none"> <li>Control the compliance with safety requirements concerning the safety of information in personal data;</li> <li>Handle complaints and make decisions related to protection of personal data;</li> <li>Register data processing systems to develop the personal data processing register.</li> </ul>	<a href="http://www.dvi.gov.lv">www.dvi.gov.lv</a>
4. Ministry of Environmental Protection and Regional Development	<p>The Ministry of Environmental Protection and Regional Development is the leading state administrative institution in the field of planning and coordination of state and regional development, local government development, spatial planning, state investment and land policy, as well as eGovernment, information society and information technology area. It integrates the previous Ministry of the regional development and local government are:</p> <ul style="list-style-type: none"> <li>Participation in state development, land policy, regional policy and spatial planning policy development;</li> <li>Coordination and implementation supervision of regional policy and spatial planning policy;</li> <li>Supervision of implementation of assignments defined by law</li> <li>in municipality working area, guidance of municipalities' development and</li> </ul>	<a href="http://www.varam.gov.lv">www.varam.gov.lv</a>

National authorities	Role and responsibilities	Website
	<p>implementation of municipalities' reform;</p> <ul style="list-style-type: none"> <li>• Organisation and implementation coordination of laws and other normative acts in regional policy, spatial planning policy and municipality working and development areas;</li> <li>• Coordination of cooperation between state administration and municipal institutions in development of electronic services;</li> <li>• Organisation and implementation coordination of information technologies in state administration in order to provide efficiency and modernisation of state administration;</li> <li>• Provision of attraction of investments in eGovernment, information society and information technology areas;</li> <li>• Supervision of state information system in Latvia.</li> </ul> <p>The Ministry of Environmental Protection and Regional Development has incorporated into its structure the Secretariat of Special Assignments Minister for Electronic Government Affairs, main tasks being:</p> <ul style="list-style-type: none"> <li>• Organize and coordinate the development and implementation of the state policy in the field of electronic government, Information Society and IT;</li> <li>• Develop different types of services and make technical and organizing infrastructure services available and easy accessible for usage;</li> <li>• Inform and educate the society so they can fully use ICTs options while using eGovernment services.</li> </ul>	
5. State Police (4 <sup>th</sup> Unit of the Economic Police Department)	Fights cybercrime and also focuses on intellectual property protection.	<a href="http://www.vp.gov.lv">www.vp.gov.lv</a>
6. Electronic Communications Office	<p>The main tasks of the Electronic Communications Office are:</p> <ul style="list-style-type: none"> <li>• The management of radio frequency spectrum and numbering to ensure their rational and effective use;</li> <li>• The technical planning the use of radio frequency spectrum and assigning radio frequencies for radio equipment operation;</li> <li>• The provision of electromagnetic compatibility and numbering services;</li> <li>• Assigning call-signs (identification) to radio stations.</li> </ul>	<a href="http://www.esd.lv">www.esd.lv</a>
7. Latvia Public Utilities Commission	<p>As a Multi-sector Regulator, the Public Utilities Commission's role is to provide users with high quality, continuous and safe public utilities for economically reasonable prices (tariffs), to stimulate efficiency and sustainable development of public utilities ensuring profitability levels consistent with the prevailing economic conditions and to promote economically justified competition in the regulated sectors. The main tasks of the Latvia Public Utilities Commission are:</p> <ul style="list-style-type: none"> <li>• Sets tariff calculation methodologies;</li> <li>• Approves tariffs for utilities;</li> <li>• Issues licenses and supervises implementation of the set conditions;</li> <li>• Supervises compliance of utilities with requirements for quality and environmental protection, technical regulations, standards;</li> </ul>	<a href="http://www.sprk.gov.lv">www.sprk.gov.lv</a>

National authorities	Role and responsibilities	Website
8. Ministry of Education and Science	<ul style="list-style-type: none"> <li>Performs dispute out-of-court settlement, etc.</li> </ul> <p>The ministry is charged with development of technological research and curriculum in Latvia. The Ministry ensures development and implementation of a policy in the fields of education, science, sports and state language promoting sustainable growth of welfare of the citizens of Latvia as educated, healthy, physically and mentally developed personalities and integrity of the society of Latvia.</p> <p>The Ministry strengthens and ensures provision of information to the public, explanation of the adopted resolutions and the link with the society by means of implementing the best practice of the administration process and transparent principles of operation of the state administration.</p>	<a href="http://www.izm.gov.lv">www.izm.gov.lv</a>
9. Ministry of Defence	The Ministry of Defence is the leading State Administration Institution in the field of defence.	<a href="http://www.mod.gov.lv">www.mod.gov.lv</a>
10. Ministry of Interior	The Ministry of Interior is the leading State Administration Institution in the field of internal affairs.	<a href="http://www.iem.gov.lv">www.iem.gov.lv</a>

### Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
11. CERT LV	<ul style="list-style-type: none"> <li>FIRST<sup>9</sup> member</li> <li>TI<sup>10</sup> listed</li> </ul> <p>As of February 1<sup>st</sup> 2011, the two CERT teams that were referenced last year have merged together into one national CERT team: CERT LV. This CERT team has its headquarters at the University of Latvia, and will be supervised by the Ministry of Transport.</p> <p>Its objectives are to:</p> <ul style="list-style-type: none"> <li>Provide quality recommendations and consultations for IT administrators in Latvia in case of security incidents;</li> <li>Provide technical support to security incidents handling, as well as recovering from their consequences;</li> <li>Co-ordinate all responses to an incident;</li> <li>Raise awareness and distribute educational materials to improve the overall knowledge of security techniques.</li> </ul> <p>CERT LV is a TI accredited team and a FIRST member, currently listed with its previous name CERT NIC.LV.</p>	<a href="http://www.cert.lv">www.cert.lv</a>

<sup>9</sup> See: <http://www.first.org/members/teams>

<sup>10</sup> See: <http://www.trusted-introducer.nl>

## Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
12. Latvian Information and Communication Technology Association – LIKTA	<p>The Latvian Information and Communications Technology Association - LIKTA - is a professional association that regroups over 80 important ICTE product and service providers and educational institutions, as well as about 100 individual professional members of the ICTE industry sector in Latvia, namely in computer hardware and software, electronics, and telecommunications infrastructure and service providers. LIKTA is involved in:</p> <ul style="list-style-type: none"> <li>• Professional education ;</li> <li>• Computer literacy ;</li> <li>• Participation in projects of national importance ;</li> <li>• International activities ;</li> <li>• Promotion of ITTE product and services sales abroad.</li> </ul>	<a href="http://www.likta.lv/en/">www.likta.lv/en/</a>
13. Internet Association of Latvia – LIA	<p>LIA represents more than 90% of Latvian Internet Service providers (ISP) and other domestic and foreign enterprises dealing with different Internet services. Their objective is to develop, secure and popularize widely accessible Internet environment in Latvia.</p> <ul style="list-style-type: none"> <li>• To consolidate for social activities legal entities and individuals operating in Latvian Internet environment;</li> <li>• To stabilize, adjust and develop Latvian Internet environment;</li> <li>• To facilitate development and popularisation of Internet, and connected sectors, in Latvia;</li> <li>• To represent its members and Internet industry;</li> <li>• To foster qualitative up growth of LIA members, to facilitate cooperation and fellowship among members, to build up industries informative base;</li> <li>• To foster Internet popularisation in society and to stimulate growth of Internet accessibility;</li> <li>• To submit proposals concerning development of Internet related legal provisions;</li> <li>• To collaborate with Internet related non-governmental organizations in different countries, promoting bilateral and multilateral exchange of comprehensive information about information technologies.</li> </ul>	<a href="http://www.lia.lv">www.lia.lv</a>
14. Information Systems Audit and Control Association (ISACA) Latvia	<p>The Information Systems Audit and Control Association (ISACA) Latvia Chapter was officially founded in 1996; however the true story started almost four years before. ISACA Latvia Chapter while being small in numbers still is working to fulfil the same mission as the international ISACA (mainly banks and audit companies) Numerous ISACA ideas have been implemented in regulatory acts and legislation (example: a need for IT auditor in each bank of Latvia), many more have been passed to legislators (example: a need for IT auditor in each governmental institution of Latvia). One of the main topics currently in focus is the new "Information System Law" in Latvia which has come into effect and now has to be implemented and adopted in real life as well.</p>	<a href="http://www.isaca.lv">www.isaca.lv</a>

Industry Organisations	Role and responsibilities	Website
15. Telecommunication Association of Latvia - LTA	LTA promotes cooperation and development between telecommunications organisations and enterprises in Latvia.	<a href="http://www.telecom.lv">www.telecom.lv</a>
16. Association of Computer Technologies of Latvia - LDTA	<p>The major goals of LDTA, Association of Computer Technologies of Latvia, are:</p> <ul style="list-style-type: none"> <li>• Representation of the IT industry in the governmental and international institutions</li> <li>• Support of the beneficial infrastructure of IT development.</li> <li>• Taking part in educational program elaboration and implementation.</li> <li>• Realization of basic approaches of Information Society.</li> <li>• Close cooperation with other associations and state's institutions in order to meet the goals and tasks desired.</li> </ul>	<a href="http://www.itnet.lv">www.itnet.lv</a>
17. Latvian Electrical Engineering and Electronics Industry Association - LEtERA	<p>LEtERA is an independent, voluntary and non-governmental public organization and unites companies, research and educational institutions registered and operating in Latvia, whose activities are related to Industry of Electronics and Electrical Engineering, Information and Communications Technology.</p> <p>LEtERA is established in order to search for solution of different problems, which are common to several sectors of ITTE branch; supports cooperation with other branch associations in Latvia, as well as related organizations of European countries:</p> <ul style="list-style-type: none"> <li>• Search for solution of different problems, which are common to several sectors of ITTE branch; supports cooperation with other branch associations in Latvia, as well as related organizations of European countries;</li> <li>• LEtERA willingly consults Latvian government and administrative body so that in the most effective and practical methods it would be possible to establish in Latvia the legislation of European Union, as well as to express the propositions for supplementation of electrical engineering and electronics and related branch legislation;</li> <li>• LEtERA facilitates the development of education and science, the foundation of new enterprises, the economical and technical development of existent enterprises, to create favourable environment for innovations, which would stimulate to make new products with high added value.</li> </ul>	<a href="http://www.letera.lv">www.letera.lv</a>

## Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
18. Institute of Mathematics and Computer Science, University of Latvia	The University of Latvia is one of the most important institutes in Latvia and, as such, offers a wide variety of studies along with a wide variety of research programs. The Institute of Mathematics and Computer Science cooperates with the Ministry of Transport by hosting the national CERT.LV team.	<a href="http://www.lu.lv">www.lu.lv</a> <a href="http://www.lumii.lv">www.lumii.lv</a>
19. Riga Technical University	The Riga Technical University is mostly a polytechnic institute. Its research facilities offer a wide variety of research programs that have an impact on the industry and the economy of Latvia.	<a href="http://www.rtuasd.lv">www.rtuasd.lv</a> <a href="http://iti.rtu.lv">iti.rtu.lv</a>
20. Institute of Electronics and Computer Science	IECS was founded as a research institution of the Latvian Academy of Sciences.	<a href="http://www.edi.lv">www.edi.lv</a>

## 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 - Guidelines and case studies, Sep. 2009, available at <http://www.enisa.europa.eu/act/ar/deliverables/2009/finorg09>
- Latvia – ENISA CERT Directory : <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/latvia>

