PUBLICATIONS 9/2016

Information Security Strategy for Finland
The World's Most Trusted Digital Business Environment

MINISTRY OF TRANSPORT
AND COMMUNICATIONS

LVM MINISTRY OF TRANSPORT AND COMMUNICATIONS

Date
19 April 2016

Title of publication

Information Security Strategy for Finland The World’s Most Trusted Digital Business Environment

Author(s)

Ministry of Transport and Communications and the development group for business with information security

Commissioned by, date

The Finnish Government's plan of action for the implementation of key projects and reforms, 28 September 2015

Publication series and number

Publications of the Ministry of Transport and Communications 9/2016

ISSN (online) 1795-4045
ISBN (online) 978-952-243-477-7
URN http://urn.fi/URN:ISBN:978-952-243-477-7
Reference number

Keywords

Digitalisation, digital business, information security, data protection, information and communication management, risk management, protection of privacy, confidentiality of communications

Contact person

Olli-Pekka Rantala, Timo Kievari

Language of the report

Other information

For the preparation of the strategy a development group for business with information security was set up on 28 September 2015. The group met 5 times and arranged a hearing on the draft of the strategy. The working group submitted its proposal for the Information Security Strategy to Ms Anne Berner, Minister of Transport and Communications, on 10 February 2016. The Minister approved the proposed strategy on 10 March 2016.

Abstract

Finland is in a good position to become known as a competent, successful and reliable country, where it is safe to take hold of the opportunities brought by digitalisation. By developing and offering services based on the utilisation of digital information, it is possible to create and accelerate economic growth. Our success depends on that we develop, assimilate and experiment with new kinds of business and earning models. This requires that we can trust on the new services, business models and market actors.

Strong grip on the development of information security expertise and market development will improve our chances to influence our role and position in the rapidly changing world order. Safeguarding this digital independence is necessary for Finland's efforts to go all out for international markets and act as a bridge builder for safe and reliable cyber environment.

The vision of the national information security strategy is that the world's most trusted digital business comes from Finland. The strategy's aims are that: 1) Finland will have a legislation that is competitive and progressive from the perspective of digital business; 2) the EU's internal market will operate more reliably than so far is the case; 3) Finnish companies will benefit from international standards as well as digital products and commodities with inbuilt information security; 4) information security and the related expertise will be investigated, measured, followed-up and developed; 5) the authorities will help communities and citizens in the improvement of information security.

The central measures supporting the realisation of the aims are described in the strategy. In addition, the need for these aims and measures is justified in the strategy's justification part.

Table of Contents

1. Introduction

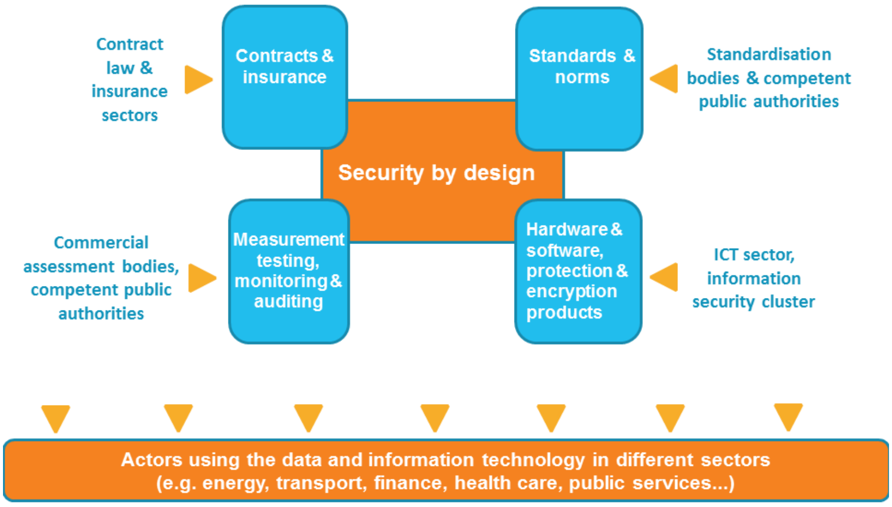
One of the key projects of Prime Minister Juha Sipilä's Government is the creation of a growth environment for digital business operations in Finland. One of the principal measures under this key project is the preparation and implementation of a national information security strategy for increasing the level of trust in the Internet and in digital practices.

The main aims and principles for the strategy work are set out in the implementation plan for the key projects. The national information security strategy is intended to focus on ensuring competitiveness and suitable conditions for exports, developing the EU's digital single market and promoting and protecting privacy and other fundamental rights. The strategy aims to bring about change whereby information security will be built into different systems, terminal devices and services by design. The strategy also deals with matters that damage trust, such as digital security incidents and large-scale invasions of privacy in communication networks.

One element of the strategy covers the implementation of the EU's Network and Information Security (NIS) Directive currently under negotiation. During this process an assessment will be made of the impact of national legislation on the opportunities of citizens and businesses to securely use digital services and business models while also managing the risks attached to handling data.

The strategy is designed to increase the availability and use of commercial data encryption and protection methods in the single market. The implementation of the strategy will also serve to develop information security features in terminal devices, operating systems, browsers, search engines, messaging applications, cloud services and other important information and communications technology goods and services. The measures in the strategy will also be used to improve the interoperability, transparency and verifiability of security features in digital goods and services. At the same time, the ability to detect and investigate information security anomalies will be strengthened. An assessment will be made of the means which Finland could use to retain companies that provide information security expertise and services that are critical for businesses in Finland.

Under the proposed EU Network and Information Security Directive, each Member State will have to prepare a national strategy setting out the framework, vision, objectives and priorities concerning network and information security at the national level. This strategy and its implementation will take account of the requirements of the proposed Directive, which is currently at the final stages of negotiation.


Contract law & insurance sectors
Contracts & insurance
Standards & norms
Standardisation bodies & competent public authorities
Security by design
Commercial assessment bodies, competent public authorities
Measurement testing, monitoring & auditing
Hardware & software, protection & encryption products
ICT sector, information security cluster
Actors using the data and information technology in different sectors
(e.g. energy, transport, finance, health care, public services...)

2. Strategic vision

Finland is in a good position to build a reputation as a highly competent, successful and reliable country where the opportunities brought by digitalisation, such as the Internet of Things (IoT), exploiting big data, and various smart technologies, can be securely taken and pursued. Developing and offering data-driven services can drive growth in the economy. Our success will depend on our capability to develop, adopt and try out new kinds of business and revenue models. The readiness to relinquish old, inefficient structures and the courage to adopt new approaches are to a significant extent dependent on the trust placed in the new services, business models and market actors.

Active participation in the development of information security expertise and markets will improve our opportunities to influence Finland’s role and position in a rapidly changing world. Securing digital independence is essential to help Finnish businesses enter international markets. It is also essential in terms of Finland’s capability to serve as an intermediator for a secure and reliable cyber environment. Furthermore, the different parties involved should come together to establish suitable conditions to ensure that one or more of the world’s leading information security companies in the future will be Finnish.

The vision set out in the national information security strategy is that:

> **“The world’s most trusted digital business environment is in Finland.”**

3. Strategic objectives and measures to achieve them

The vision set out in the strategy can be achieved by improving information security and the reliability of business reliant on it in a consistent manner using a variety of different means. Advances can be made especially by means of legislation, agreements, technologies and business models.

The objectives set out in the strategy are as follows:

1) Finnish legislation will incorporate both competitive and forward-looking provisions from the perspective of digital business;
2) the EU's digital single market will operate in a more dependable manner than at present;
3) Finnish companies will benefit from international standards and there will be digital goods and services available on the market which are safe and secure by design;
4) information security and related know-how will be researched, measured, monitored and developed;
5) the authorities will help businesses and citizens to improve their information security.

Each objective and the main measures supporting its achievement are explained in more detail in the sections that follow below.

3.1 Finnish legislation will incorporate both competitive and forward-looking provisions from the perspective of digital business

National legislation will establish suitable conditions for business activities to be as competitive as possible. Finland will be an attractive location for investment based on processing and utilising data. For companies seeking to utilise digital opportunities, Finland will stand out as a reliable location for establishing a business.

MEASURES:

- In connection with preparing and streamlining legislation on the digital environment, especially data processing and information security, the impact of these statutes on information security and businesses will be assessed.[1]
- The NIS Directive will be implemented, securing companies' capabilities of including in their risk management programmes the new information security obligations required. To ensure this, a working group to assist in the implementation will be established to assess the adequacy of existing national legislation in each sector within the scope of the directive.[2]
- Every effort will be made in amending national legislation as required by the EU's Data Protection Regulation, to avoid incorporating any additional burden that could adversely affect the competitiveness of businesses.[3]
- Attention will be given to ensuring that development of the EU legislation concerning the responsibilities of electronic communications service providers is technology and operator neutral (obligation to respect privacy and information security when conveying messages).[4]
- In cyber security development work, all means will be used to promote and protect user rights, such as the rights to privacy and confidentiality of communication, in electronic services and the online environment.[5]

[1] Responsibility: all ministries

[2] Responsibility: Ministry of Transport and Communications, Ministry of Employment and the Economy, Ministry of Finance, Ministry of Social Affairs and Health, Ministry of the Environment

[3] Responsibility: Ministry of Justice and other ministries

[4] Responsibility: Ministry of Transport and Communications

[5] Responsibility: Ministry of Defence, Ministry of the Interior, Ministry of Justice, Ministry of Transport and Communications, Ministry of Finance

3.2 The EU's digital single market will operate in a more dependable manner than at present

Finland will strive to reduce the country risks within the EU and the international community in order that the free flow of data can be secured without compromising the fundamental rights of citizens and the objects of legal protection of businesses. Finland's goal is to achieve a common approach within the EU and the international community to the conditions and limitations of state interference in the privacy or information security of a person in another State. In drawing up treaties, Finland will give particular attention to the effects of such agreements on Finnish companies that produce and use information security goods and services.

- **MEASURES:**
- Finland will acknowledge the objectives of this strategy in the implementation of the EU's strategies for a digital single market and cyber security.[6]
- Finland will actively seek to ensure that the objectives of this strategy are taken into account in the activities of the European Union Agency for Network and Information Security (ENISA).[7]
- Finland will take the objectives of this strategy into account in the preparatory work for the declaration to be issued at the OECD Ministerial Meeting in Cancun during 2016.[8]
- The objectives of this strategy will be taken into account in the coordination of the foreign policy dimensions of cyber security and preparation of treaties binding on Finland.[9]
- Finland will seek to ensure that the objectives of this strategy are taken into account in the European Commission's trade negotiations.[10]

[6] Responsibility: Ministry of Transport and Communications, Ministry for Foreign Affairs, Ministry of Employment and the Economy, Ministry of Finance

[7] Responsibility: Ministry of Transport and Communications, Finnish Communications Regulatory Authority

[8] Responsibility: Ministry of Transport and Communications, Ministry of Employment and the Economy

[9] Responsibility: Ministry for Foreign Affairs

[10] Responsibility: Ministry for Foreign Affairs, Ministry of Transport and Communications

3.3 Finnish companies will benefit from international standards and there will be digital goods and services with inbuilt information security available on the market

Goods and services with inbuilt security features will be developed, made available and used in Finland. Finland will be able to offer terminal devices, operating systems, browsers, search engines, messaging applications, cloud services and other key digital goods and services whose information security features are so comparable that their transparency, efficiency and verifiability will be easy to assess. Finland will have the world's most advanced commercial services for enabling companies to measure and reduce (including underwriting) information security risks that could cause financial loss to their business. Finland and the EU will adopt standards that make it easier to choose a reliable contractual partner in terms of information security. These objectives will also be extended to developing the Internet of Things (IoT), both nationally and internationally.

MEASURES:

- Trust in digital services and electronic transactions will be enhanced by launching a nationwide trust network for electronic identification. The aim is that the different operators can more easily use strong electronic identification and trust the identification data transmitted by others in the network. As part of the National Service Architecture Programme for the public sector, the State will develop a centralised service for the electronic identification of citizens.[11]

- Conditions favourable for the creation of anonymisation services will be developed in cooperation between the public and private sector to help businesses manage the information security risks related to personal data processing.[12]

- A study will be made of the user terms and data protection features of the most common terminal devices, operating systems, Internet browsers, search engines and messaging applications in regard to the ability of users to protect the data within their own business activities or in other activities.[13]

- A study will be made of the need – from the user's perspective – for certification of various data security and protection features and the impact of such certification on the trust placed in digital goods and services. The importance of certification and standardisation bodies to hardware and service providers in the ICT sector and their customers will be also studied.[14]

[11] Responsibility: Ministry of Transport and Communications, Ministry of Finance, Population Register Centre

[12] Responsibility: Ministry of Transport and Communications, Ministry of Finance, Population Register Centre, Data Protection Ombudsman

[13] Responsibility: Finnish Communications Regulatory Authority, Data Protection Ombudsman, Ministry of Finance

[14] Responsibility: Ministry of Transport and Communications, Finnish Communications Regulatory Authority, Finnish Standards Association SFS

3.4 Information security and related expertise will be researched, measured, monitored and developed

The costs of information security risk management for businesses will be researched and monitored in Finland. R&D investments related to improving the information security of the goods and services that businesses produce will also be studied. The possibilities for including data analysis and cryptology studies and research in the teaching programmes of different educational and research institutions and in other research programmes will be assessed.

MEASURES:

- A situation report will be made of the financial impacts of information security incidents and the costs of preventive measures taken against these – including financial loss and damage caused by data and communications offences.[15]
- A survey will be made of Finnish information security projects that could receive funding from the European Commission as part of its cyber research programme to be set up in 2016.[16]
- As part of the research and development activities supporting Government decision-making, means will be sought for improving the reliability of digital services and business models.[17]
- The contribution of information security products and their development to net sales in the ICT sector will be monitored. Principal responsibility: Federation of Finnish Technology Industries, Finnish Information Security Cluster
- The need for data protection and security experts experienced by companies in Finland will be researched. A study will be made of the means for improving the availability of experts. Sufficient resources for training and education in information security will be secured.[18]
- A series of information security events ('hackathons') will be arranged, helping to identify national information security experts and to support networking among them.[19]

[15] Responsibility: Ministry of Transport and Communications, Ministry of the Interior, Ministry of Finance

[16] Commission's programme for improving the availability of European information security products through cooperation between the private and public sectors. Responsibility: Finnish Information Security Cluster, Federation of Finnish Technology Industries, Ministry of Transport and Communications, Ministry of Defence

[17] On 3 December 2015 the Government approved an analysis, assessment and research plan to support Government decision making, including a project to investigate how the reliability of digital goods and services and business models can be improved. Responsibility: Prime Minister's Office, Ministry of Finance

[18] Responsibility: Ministry of Education and Culture, Ministry of Employment and the Economy, Finnish Funding Agency for Innovation (Tekes)

[19] Responsibility: Finnish Communications Regulatory Authority, companies, Ministry of Employment and the Economy, Finnish Funding Agency for Innovation (Tekes)

3.5 The authorities will help businesses and citizens to improve their information security

The authorities will provide assistance and support for companies in integrating information security in their business, for example by collecting and sharing information on the management of information security risks. Companies will have good opportunities to participate in the standardisation of goods, services and trust enhancing features, with the support of the authorities and relevant organisations.

MEASURES:

- The availability of commercial and public services for detecting hidden information security risks, assessing the unwanted effects of these risks and reducing these risks by sharing information will be examined.[20]
- A situation report on information security will be maintained through confidential information exchange between the Finnish Communications Regulatory Authority, companies and other entities.[21]
- A working group of authorities and businesses will be established to improve the prevention and countering of offences targeting companies. The group will focus on certain issues, including combating cybercrime.[22]
- With suitable interpretation practices and transparent procedures and by offering services, the authorities will, within the scope of their powers, support the creation of new trust-enhancing business models based on data processing.[23]
- A national network supporting the participation of Finnish companies in standardisation work will be formed to promote the commercial availability, use and export of information security services and goods that improve the confidentiality of communications.[24]
- A study will be made of whether there is demand for information security products and services whose supply or use could be governed solely by Finnish or EU legislation. An assessment will be made of how it would, if necessary, be possible to keep these services in Finland, for example by means of State ownership.[25]
- Business representatives and the principal authorities involved with this strategy will come together as a network to monitor its implementation. The ministries will incorporate the measures required in the strategy into their own operational and financial plans. A summary of the implementation will be provided to the network.[26]

[20] Responsibility: Ministry of Transport and Communications, Finnish Communications Regulatory Authority, National Emergency Supply Agency, Ministry of Finance
[21] Responsibility: Finnish Communications Regulatory Authority, companies, Ministry of Finance
[22] Responsibility: Ministry of the Interior, companies
[23] Responsibility: competent public authorities
[24] Responsibility: Finnish Communications Regulatory Authority, Finnish Standards Association SFS
[25] Responsibility: Prime Minister's Office
[26] Responsibility: Ministry of Transport and Communications and other ministries