

Creating a Safer Information Society

***National Information Security Advisory Board report
submitted to the Government on 14 December 2004***



MINISTRY OF TRANSPORT
AND COMMUNICATIONS FINLAND

Creating a Safer Information Society

National Information Security Advisory Board report
submitted to the Government on 14 December 2004

Programmes and strategies 3/2005
Ministry of Transport and Communications

ISSN 1457-747X (printed version)
ISSN 1795-4037 (electronic version)

ISBN 951-723-487-2 (printed version)
ISBN 951-723-488-0 (electronic version)

Graphic design
Workshop Pälviä

Printed by
Vammalan Kirjapaino Oy 2005

Photographs
Cover photograph: Heikki Pälviä
Other photographs: Antero Aaltonen, Tero Pajukallio, Heikki Pälviä, Hannele Sartjärvi

On-line publication at www.mintc.fi

Creating a Safer Information Society

*National Information Security Advisory Board report
submitted to the Government on 14 December, 2004*

Message from Minister of Transport and Communications Leena Luhtanen at the handover of the Advisory Board report on 14 December 2004	4
National Information Security Advisory Board	6
The Advisory Board's progress report and its proposals to the Government	8
Government Resolution on the National Information Security Strategy, 4 September 2003	14
1. Promotion of national and international information security cooperation	16
1.1. National Information Security Advisory Board	17
1.2. International cooperation	18
1.3. The importance of trust and information security in the New Economy	20
1.4. Operating conditions needed for the different actors at national level	21
2. Promotion of national competitiveness and the operating potential of Finnish information and communications operators	22
2.1. Programme on trust and information security in electronic services	23
2.2. Corporate information security awareness	25
2.3. Convenient and compatible products and innovative areas for development	27
2.4. Harmonizing public-sector information security procedures	29
2.5. Impact assessment of legislation	32
2.6. Information security and privacy protection in biometric identification	34
3. Improving information security risk management	36
3.1. Assessing and more effectively combating information security risks	37
3.2. Analysis of national information security risks	41
3.3. Methods for analysing vulnerability to information security risks	44
3.4. Committee on Information Security in Critical Infrastructure	46
4. Safeguarding fundamental rights and protecting the nation's knowledge capital	48
4.1. Ensuring fundamental rights	49
4.2. Protection of national knowledge capital	51
4.3. Cybercrime as an information security problem	53
5. Increasing information security awareness and competence	56
5.1. Charting and developing information security awareness and competence	57
5.2. Improving people's information security awareness	59
5.3. Information security awareness in public administration	60
5.4. Certificates	62
5.5. National Information Security Day 2005	64
Actors in the Finnish Information Security Sector	68

Message from Minister of Transport and Communications Leena Luhtanen at the handover of the Advisory Board report on 14 December 2004

The Government Resolution on the National Information Security Strategy, which was adopted in September 2003, has attracted considerable attention here in Finland and also internationally. The content of the Resolution was based on extensive preparatory work by the Advisory Board's predecessor in 2001–2003, in cooperation with the public and private sectors and with users. No party interested in participating was excluded.

The far-reaching vision embodied in the Resolution is to create **a safer information society in Finland**. The actions outlined in the National Information Security Strategy are designed to enhance the different actors' trust in the information society. The focus of the Strategy is on combating threats to information security in both normal and exceptional circumstances, and making use of the opportunities associated with information security improvements. Finland is not only a major consumer of information society services but also a significant producer and exporter of information security products. The Strategy seeks to establish common objectives and guidance on information security for the public sector, the corporate sector, other bodies and organizations and the general public. Under the National Information Security Strategy, a safer information society is possible through national and international cooperation within the sector, improvements in the operating potential for Finnish ICT companies, improved management of information security risks, ensuring that fundamental rights and the nation's knowledge capital are safeguarded, and increasing the level of information security awareness and competence.

It is absolutely **essential that the strategy be transformed from words into decisive action**. When setting up the National Information Security Advisory Board, the tasks I allotted to it included monitoring the Strategy's implementation and the coordination of the various measures involved. The Board's membership represents strategic decision-making interests from all sectors of society. One of the Board's key tasks has been to

detect, from even the weakest of signals, which particular measures are needed for maintaining and enhancing trust and confidence in the information society.

A society based on the use of information and communication technologies has new kinds of vulnerabilities. The more advanced the information society, the more important it is to consider the potential new threats. Information security has tended to be viewed largely as a technical challenge. However, the changeover to an ICT-based economy means that **information security is primarily an economic and political challenge**. Only very recently have we begun to look systematically at the significance of economic factors for information security. An economic analysis is often more successful than a purely technical one in explaining why information security fails or why there is insufficient contingency for it. The fact is that the standard of information security is typically determined by the resources available for it within a business rather than by what is actually needed for absolute protection against the risks. Investing in information security is clearly a cost and will have an impact on competitiveness. However, anyone who would ultimately bear the cost of inadequate information security will also be more ready to invest in information security. An understanding of this raises the political significance of information security and the level of interest in it.

Information security is not of intrinsic value in itself; its importance is determined only in relation to the benefit derived from it or the problems caused by its neglect. Political guidance must be based on a realistic view of the importance of information security for the functioning of society. The risks and the consequences must be understood, and information security policy must focus on preventive measures. **New sectors of the economy will potentially have more to lose than the more traditional sectors**. Even so, nobody would consider computers or the Internet to be completely secure any more. In the mobile



phone industry, for example, the image of the entire sector would suffer greatly if viruses and worms were to find their way into phones from unsecured software updates. There is thus good reason to hope and believe that the mobile phone industry will protect itself against future threats more successfully than the PC industry.

In the development of national policy on information security Finland is at the forefront in Europe. In this we have something to offer other EU members, too. In our preparations for Finland's EU Presidency in autumn 2006 we have therefore expressed the wish to the Commission that the EU should start work on drafting a Union-wide information security strategy along the lines of the Finnish model. The EU has already set up a separate agency, the European Network and Information Security Agency (ENISA), for dealing with its work on information security policies. Political guidance will not come from the agency, however. What the EU needs is a common view of how the competitiveness of its communications sector can be improved in information security terms. Furthermore, the Union must be fully able to participate in combating global information security threats, such as spam e-mail and virus epidemics. This requires political input.

The development of national information security policy must be driven by a political need. **Information security threats are a threat to the very foundation of a modern information society.** Above all, these threats affect people's confidence in electronic services. If this is damaged, the use of such services will diminish. The consequences of this have not yet been seen on a large scale, but the seeds of doubt have been sown. Information security violations have so far been mainly annoyances that have caused extra inconvenience and trouble. If the present trend continues, it is only a matter of time before something more serious occurs.

The National Information Security Strategy has proved very useful in promoting cooperation between the various actors in the information security sector. Considerable effort has also been

made to ensure that a realistic and truthful picture is presented of the present state of information security and that future threat scenarios are assessed. It is well known that last year, 2003, was the worst so far for the incidence of malicious software. In the autumn, for example, many Finns were astonished to discover that their home PCs had been the source of hundreds of thousands of spam e-mails sent out around the world. The current year has not been any easier, and worse is sure to come. There are many reasons for this, such as the continued integration of different systems and their connection to open communications networks, allowing malicious software to spread more easily. Such software is also becoming more intelligent. In addition, development of the information society is progressing at all levels in Finland and elsewhere, and **we are becoming ever more dependent on our information systems.** A lot remains to be done, but we are off to a good start.

On behalf of the Government, I would like to thank the Advisory Board, its Secretariat and every organization and individual that participated in the assembly of the Strategy for their valuable input. The material resulting from one year's work is already immense in both quantity and value. I have also noted that you have devoted your time and expertise to this collective effort without any separate recompense. Working for a common cause is a unifying experience. You have successfully launched a great many projects which allow us to shed light on future threats and opportunities. We have to be able to look ahead a little further and a little more quickly than our international competitors. **You are all helping reinforce the competitiveness of Finland's information society,** and you are doing it very well!

I very much appreciate that, proceeding across a broad front, you have identified the information security threats of greatest significance for the information society and have then resolutely set about establishing timetabled priority areas on the basis of that information. I hope that your future work will focus on finding practical solutions to the many challenges, existing and new. As I have very strongly stressed already, the growth in the national importance of information security means that **even the practical work of the Advisory Board must be seen ever more emphatically against the background of public policy.** This report provides a good account of the necessary course.

I am very satisfied with the work you have done and I wish you all a successful end to 2004, a Peaceful Christmas and great accomplishments in 2005.

14 December 2004

Leena Luhtanen, Minister of Transport and Communications

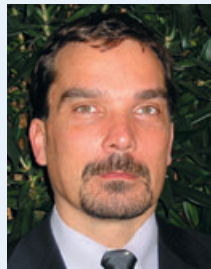
National Information Security Advisory Board



Harri Pursiainen
Chair, Director-General
Ministry of Transport and
Communications



Kristiina Pietikäinen
Deputy Chair, Director of Unit
for E-commerce and Data
Security, Ministry of Transport
and Communications



Timo Kekkonen
Director-General
Ministry of Trade and Industry



Arvo Jäppinen
Deputy Director-General
Ministry of Education



Marco Krogars
Director-General
Ministry of Defence



Reijo Naulapää
National Police Commissioner
Ministry of the Interior



Jorma Karjalainen
Director-General
Ministry of Finance



Mika Purhonen
Director-General
National Emergency
Supply Agency



Marita Wilska
Consumer Ombudsman
Consumer Agency



Markku Koli
Deputy Chief of Operations
The Finnish Defence Forces



Reijo Aarnio
Data Protection Ombudsman
Office of the Data
Protection Ombudsman



Rauni Hagman
Director-General
Finnish Communications
Regulatory Authority (FICORA)



Hannele Pohjola
Chief Policy Adviser
Confederation of
Finnish Industries (EK)



Reijo Svento
Managing Director
Finnish Federation for
Communications and
Teleinformatics (FICOM ry)



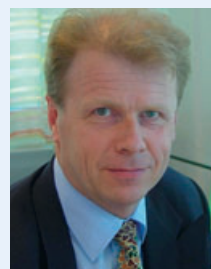
Jouni Keronen
Chief Information Officer
Fortum Corporation



Risto Siilasmaa
CEO
F-Secure Corporation



Leena Linnainmaa
Deputy Director
The Central Chamber of
Commerce



Martti Mehtälä
General Manager
Microsoft Oy



Elise Lepinsalo-Harju
Senior Manager
Nokia Group



Bo Harald
Executive Vice President
Nordea Bank Finland Ltd



Arto Vainio
CEO
SSH Communications
Security Corporation



Ilkka Hiidenheimo
CEO
Stonesoft Corporation



Lauri Virkkunen
General Manager
Vattenfall Oy

Advisory Board Secretariat



Secretary General
Juhapekka Ristola
Ministerial Adviser
Ministry of Transport and
Communications



Päivi Antikainen
Ministerial Adviser
Ministry of Transport and
Communications



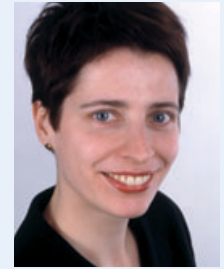
Keith Bonnici
Senior Technology Adviser
National Technology
Agency of Finland



Nora Elers
Communications Manager
Finnish Federation for
Communications and
Teleinformatics (FiCom ry)



Sanna Helopuro
Ministerial Adviser
Ministry of Transport and
Communications



Mari Herranen
Senior Officer
Ministry of Transport and
Communications



Ilkka Kananen
Deputy Director General
National Emergency
Supply Agency



Kristiina Klemetti
Communications Manager
Finnish Federation for
Communications and
Teleinformatics (FiCom ry)



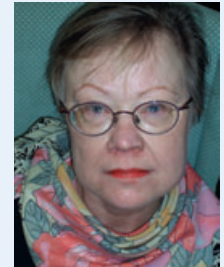
Kaarlo Korvola
Head of Information
Management
Ministry of the Interior



Jaana Lappi
Senior Adviser
Ministry of Trade and
Industry



Timo Lehtimäki
Head of Information Security
Finnish Communications
Regulatory Authority (FICORA)



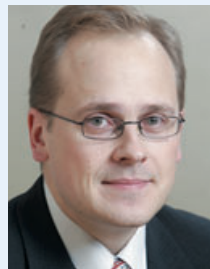
Terttu Mellin
Ministerial Secretary
Senior Officer
Ministry of Finance



Kirsi Miettinen
Special Adviser
Ministry of Transport and
Communications



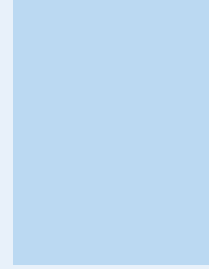
Markku Suvanen
Senior Adviser
Ministry of Education



Juha Perttula
Ministerial Adviser
Ministry of Transport and
Communications



Tapio Virkkunen
Ministerial Adviser
Ministry of Transport and
Communications



Sari Kajantie
Chief Superintendent
National Bureau of
Investigation

The Advisory Board's progress report and its proposals to the Government



What is expected of the Advisory Board?

Beginning its work in spring 2004, the National Information Security Advisory Board has had the task of ensuring coordination of the actions implementing Finland's National Information Security Strategy and of monitoring the Strategy implementation through to the end of its term in May 2007.

The Advisory Board is required to submit an annual report to the Government on the implementation of the Strategy and on the need to update it. The Board must also provide a broadbased forum for the purpose of improving cooperation between the different actors and organizations involved in information security. Through its Action Plan to Implement the National Information Security Strategy, the Board is required to set out the main principles of its work and guidance on detailed monitoring of the measures taken.

The Board's view on progress to date

The Advisory Board finds that Finland is firmly at the forefront of developments in information security. It is the first country in the world to have drawn up a national information security review, and the first in Europe to draft an information security strategy for society at large and to enact detailed legislative provisions on the careful filtering of harmful communications and malicious software. In the Board's view, Finland must ensure its place among the leading countries in information security because it is among the frontrunners in information society development in general. For an information society, the threat to information security is a very real one, which is not the case for societies which are predominantly agricultural or industrial.

While the European Information Security Award granted for the Strategy and the other results achieved are gratifying, they are no excuse for complacency in view of the coming challenges to be met in developing Finland's information society.

In February 2004, the Board adopted an Action Plan to implement the National Information Security Strategy as an aid to ensuring projects meet the objectives set by the Government. In its work, the Board, together with its Secretariat, has sought to find new methods for approaching information security issues in a transparent and customer-focused way and with an understanding of the instrumental value of information security in building up confidence.

This report describes the progress on projects already under way and the objectives for the coming year, and gives the Secretariat's assessment of the impact of the different measures in isolation and in combination with other projects. There are altogether more than 20 projects in progress, most of which deal with complex and previously poorly understood phenomena. The Advisory Board itself has become an acknowledged discussion and coordination forum for discussing complex and challenging national projects and solutions; an increasing number of ministries and internationally recognized companies have sought to be involved with the work of the Board.

The aims of the various projects include establishing the right basis for defining information security more clearly as an economic phenomenon contributing to an improvement in the nation's competitiveness. This is the key objective underlying the launch of the project entitled *Programme on information-secure electronic services*, which focuses on the development of new secure electronic services. In projects aimed at enhancing the information security awareness of companies, information security has been seen as an instrument for increasing corporate confidence in the opportunities for using information and communications technology; companies making extensive use of ICT are able to gain a competitive edge and improve their efficiency. Further progress towards the same goal has also been achieved through public technology funding for the development of

new information security products and services for a number of Finnish information security companies and research organizations.

In the work to facilitate the development of services that use biometric identification it has become clear that the different actors involved inevitably need to know more about which information security factors they should consider in their biometric services and systems. Similarly, in regard to assessment of future options it has been noted that confidence in the Internet and in ICT in general can falter if there is a deterioration in information security. It is increasingly apparent that tackling these problems requires long-term measures and perspectives. Among the measures needed is the creation of a system for analysing the status of national information security. To this end, a project has been set up entitled *Analysis of national information security risks*, the impact of which should be visible in 2004–2005 in the form of an increase in information security awareness, in particular, and thus a reinforcement of the national information security culture.

The survey of the nation's knowledge capital has provided a better understanding of which elements of these valuable resources should be protected through collective measures and how such protection can be improved. At the same time, different organizations have begun to realize the importance of their knowledge capital and the necessity of protecting it. The aims of the project for preventing information security crime are to ensure the readiness for tackling an increase in serious and organized crime perpetrated over information networks, to make sure that computer-related crime (cybercrime) can still be investigated effectively in the future, and to encourage those who maintain information systems to protect their own and their customers' systems from known malicious software and targeted attacks.

The aim of the projects for surveying general awareness of information security issues is to form a realistic picture of information security awareness and competence so that the necessary measures can be targeted as accurately as possible. Within this overall framework, National Information Security Day 2004 was a resounding success in terms of its aim to improve ordinary Internet users' awareness of hidden information security threats and the means by which they can be avoided. The same event in 2005 looks set to succeed as well or better. Besides improving the general public's awareness, the project is expected to be especially useful in developing the information security awareness of schoolchildren.

On various matters it has been possible to disseminate more widely the results of previous work. At the same time, a number of information security 'backwaters' not previously investigated have also been found. While developing information security at a technical level, it has proved difficult in many projects to ensure the necessary focus on awareness and financing. Nevertheless, information security and its

different aspects have become subjects of national significance.

The Advisory Board considers that the progress made with individual projects across a broad front in the initial months has been enough to enable the different elements of information security to be identified. The inclusion of professionals and experts in the projects has been significant: almost two hundred key actors have participated in the steering groups of over 20 different projects, which is an indication of how well the Strategy has been received during the first year of its implementation.

To ensure sufficient progress in implementing the Strategy, it has been necessary to select a number of priority projects and to ensure that they are timetabled carefully and given the necessary support. It also remains important to try and achieve further concrete results that can be objectively measured. The Board's different projects have attracted a reasonable amount of publicity and, with carefully targeted communications, media coverage can be ensured in the future, too. The objectives, responsibilities and means for publicity and communications are set out in the communications plan.

The Board's proposals

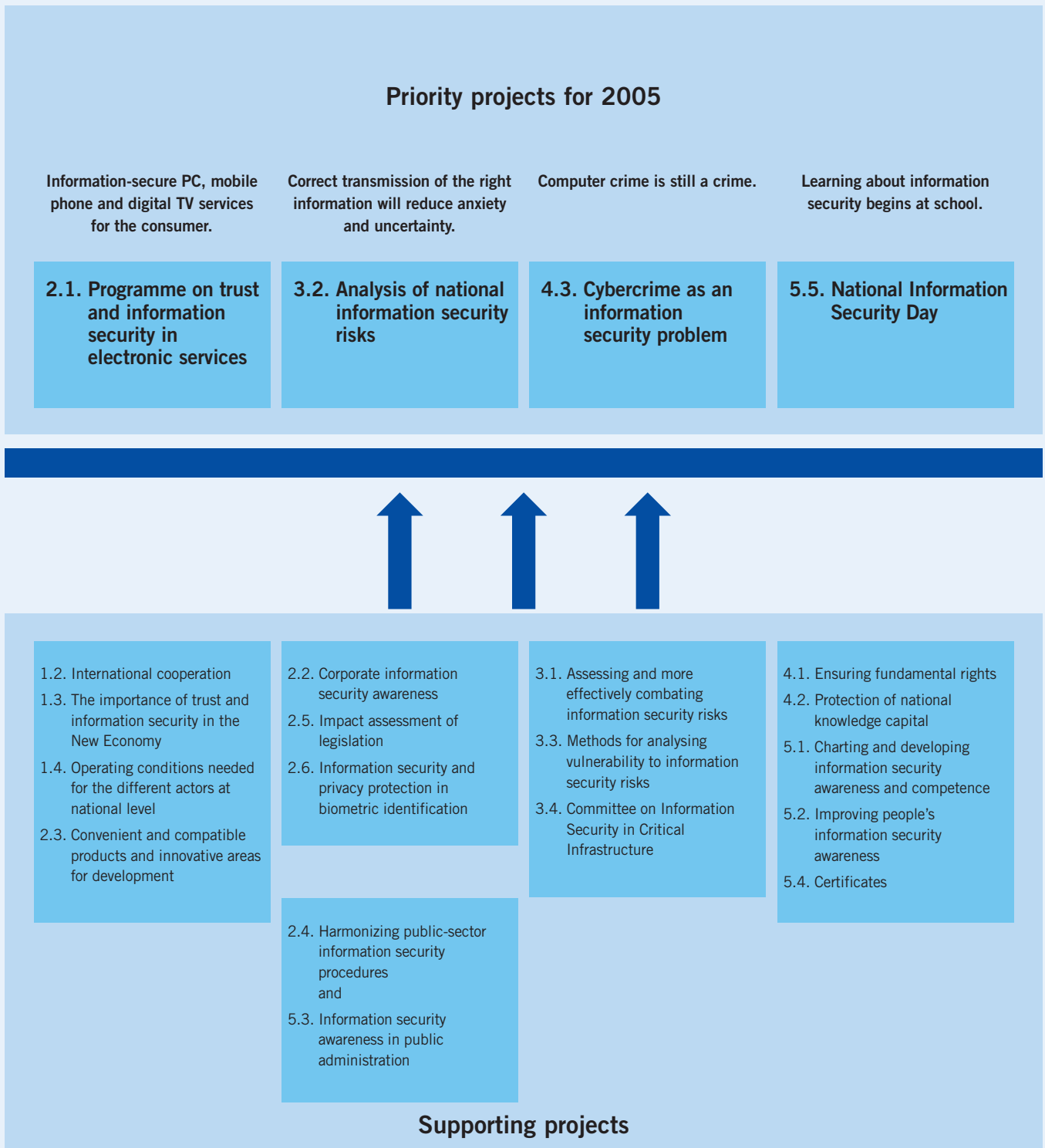
The Advisory Board considers that the following projects should be given priority in 2005 in order to ensure the effective implementation of the National Information Security Strategy:

- 1 Programme on information-secure electronic services**
Guiding principle: *"Promoting information-secure PC, mobile phone and digital TV services for the consumer."*
- 2 Analysis of national information security risks**
Guiding principle: *"Correct transmission of the right information will reduce anxiety and uncertainty."*
- 3 Cybercrime as an information security problem**
Guiding principle: *"Computer crime is still a crime."*
- 4 National Information Security Day**
Guiding principle: *"Learning about information security begins at school."*

At the same time, the other projects are arranged into groups, each supporting one of the above priority projects. The priorities for the following year, 2006, will need to be determined separately. The choice of projects is based on a consideration of which project timetables allow for achievement of the most concrete results in the year ahead. Some projects will clearly be of longer duration or more relevant at a later stage. The selection is not a question of placing values on projects or the work done in them.

The Board feels it is essential that new avenues for promoting national productivity and competitiveness through information security measures be established continuously and without delay in order to ensure the effective development of Finland's information society.

Creating a Safer Information Society



The Advisory Board considers it important to select priority areas for its work in 2005 to ensure the effective implementation of the National Information Security Strategy. At the same time, the other projects are arranged into groups, each supporting one of the priority projects.

Signatures of Advisory Board members and Secretary General, 14 December 2004



Harri Pursiainen
Chair, Director-General, Ministry of Transport and Communications



Hannele Pohjola
Chief Policy Adviser, Confederation of Finnish Industries (EK)



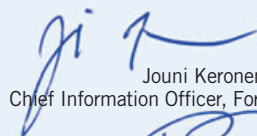
Kristiina Pietikäinen
Deputy Chair, Director of Unit for E-commerce and Data Security
Ministry of Transport and Communications



Reijo Svento
Managing Director
Finnish Federation for Communications and Teleinformatics (FiCom ry)



Timo Kekkonen
Director-General, Ministry of Trade and Industry



Jouni Keronen
Chief Information Officer, Fortum Corporation



Arvo Jäppinen
Director-General, Ministry of Education



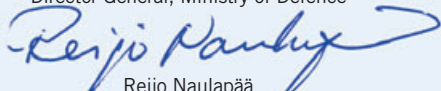
Risto Siilasmaa
CEO, F-Secure Corporation



Marco Krogars
Director-General, Ministry of Defence



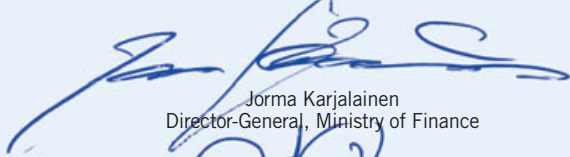
Leena Linnainmaa
Deputy Director, The Central Chamber of Commerce



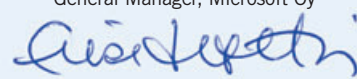
Reijo Naulapää
National Police Commissioner, Ministry of the Interior



Martti Mehtälä
General Manager, Microsoft Oy



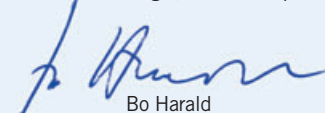
Jorma Karjalainen
Director-General, Ministry of Finance




Elise Lepinsalo-Harju
Senior Manager, Nokia Group



Mika Purhonen
Director-General, National Emergency Supply Agency



Bo Harald
Executive Vice President, Nordea Bank Finland Ltd



Marita Wilska
Consumer Ombudsman, Consumer Agency



Arto Vainio
CEO, SSH Communications Security Corporation



Markku Koli
Chief of Operations, The Finnish Defence Forces



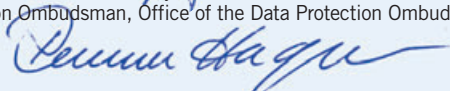
Ilkka Hiidenheimo
CEO, Stonesoft Corporation



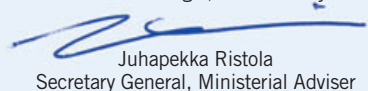
Reijo Aarnio
Data Protection Ombudsman, Office of the Data Protection Ombudsman



Lauri Virkkunen
General Manager, Vattenfall Oy



Rauni Hagman
Director-General, Finnish Communications Regulatory Authority (FICORA)



Juhapekka Ristola
Secretary General, Ministerial Adviser
Ministry of Transport and Communications

Overview of information security



Developments in information security in Finland during 2004 were mixed. On the positive side, there was a general improvement in information awareness, particularly the awareness among households and businesses of the need for anti-virus software, a personal firewall and software updates. Nevertheless, the deficient basic knowledge of network services among users remains a key challenge.

Despite an increase in information security awareness, there has been no decrease in the problems experienced. Software vulnerabilities, for instance, have been discovered at an ever more frequent rate, and the range of potential problems as a whole has, in practice, continued to grow. Malicious software is also able to exploit these vulnerabilities over a shorter cycle than before, which imposes special challenges for software manufacturers.

In regard to legislative measures, Finland achieved a significant milestone with the entry into force of the Act on the Protection of Privacy in Electronic Communications. This gives the authorities and the different actors in the sector much clearer guidance on improving information security in networks. On the basis of the legislation and in cooperation with operators, the Finnish Communications Regulatory Authority (FICORA) began preparing new regulations on the reliability and information security requirements for e-mail and Internet connection services.

Malicious software

A particularly extensive “virus war” was waged between malicious software writers in spring 2004. A considerable number of viruses from writers representing Bagle, Netsky and Mydoom malware were found in networks. The motives of those sending out such software have clearly changed. The purpose is no longer to destroy infected information systems. Instead, the main aim is currently to gain control of the infected system. Once controlled, the system can be used for such purposes as searching for new vulnerable targets, sending/forwarding spam e-mail, as a platform for DoS (denial of service) attacks or as a web server incorporating hoax pages for use in “phishing” activities.

In “phishing”, the aim is to get the user to divulge information to a network service that appears to be genuine but is in fact fraudulent, being designed to collect credit card data, service registration data or personal data for criminal purposes. During 2004, there were also cases of malicious software that collected financial data directly from an infected system by observing entries made by the user. Vulnerable home PCs are still among the systems most widely exploited.

The most significant of the lesser reported malicious software included various types of bot malware (e.g. Phatbot, SDbot, Agobot). Bot malware is able to connect with command servers that use Internet Relay Chat (IRC) protocol, thus allowing the attacker to send commands to an infected information system. Information systems infected with the malware are then formed into botnet networks. A single botnet typically comprises between several hundred and several thousand, or even tens of thousands, of infected systems. Typical of botnets is that the malicious software spreads very rapidly, before the anti-virus software manufacturers can react. Those spreading bot malware are also able to make sure it goes undetected by testing it against different anti-virus software.

During 2004, several major Finnish organizations found they had a bot infection in their workstation network. A typical infection route was a portable computer transported between home and work. The security of portable computers should therefore be given particular attention. According to information received by FICORA's CERT-FI group, in the last six months of 2004 the number of Finnish systems infected with bot malware was continuously about 1,500–2,000. The CERT-FI estimate of the total number of information systems infected with all types of malware is 2,500–3,500. The majority of these are, it seems, in home PCs with broadband connections.

Malware infection routes have typically been e-mail attachments and operating system vulnerabilities at network

interfaces. During 2004, a significant new infection route emerged in the form of methods that utilize browser vulnerabilities in websites created for malicious purposes.

Spam e-mail

In 2004, the amount of spam e-mail increased at a steady rate without any dramatic changes. The same can also be said of the difficulties encountered in trying to detect spam. Spam messages now account for a very considerable proportion of all e-mails. Useful e-mails in fact account for less than half of the total, and this proportion can be reduced significantly during loading peaks, such as spam attacks, which is also detrimental to operators. Spamming has not, however, led to major problems in the operation of e-mail services in Finland.

Spamming has been strongly associated with the selling of illegal copies of computer software, traditional hoax correspondence and phishing. It is an ever growing problem, and it seems that spam e-mail, malicious software and organized cybercrime are becoming more and more intertwined. The most visible evidence of this is the very sharp growth in phishing aimed at unauthorized use of web service users' financial data, especially in the UK and the United States. There is no evidence that phishing has appeared in Finland yet, but the situation needs to be closely monitored. Phishing is, however, only a small element in the criminal activity targeted at networks.

Software vulnerabilities

During 2004, attention was focused especially on the vulnerabilities of browser software. The vulnerabilities in imageprocessing software have been another key area, emerging strongly at the end of the year. In both cases the aim is to bypass anti-virus software and firewalls. This increases the importance of having software updates as part of information security management. The time between discovering vulnerabilities and exploiting them is continuously decreasing, and the vulnerabilities most frequently exploited, according to the cases reported to CERT-FI, are accessed using automatic attack tools.

Outlook

Despite the growing problems, the Internet is not yet falling apart, but continuous development work is essential in order to weed out the undesirable phenomena. CERT-FI predicts that the development of bot malware will continue.

Among the security violation trends, the sharp increase in violations targeting financial gain is likely to continue. In efforts to deal with threats from the Internet, it remains essential to use a

firewall and secure versions of software. This particularly concerns the vulnerabilities found in the Microsoft Windows operating system and the Microsoft Internet Explorer browser.

Statistics on information security

The computerization and networking of Finnish households appears to have reached saturation point. The information security risks are nevertheless growing because the number of broadband connections is increasing rapidly. An increasing number of households are also buying portable computers, which represent a greater information security risk than PCs because they are also used outside the home. USB flash drive storage devices are a new information security problem, because they are used to store information that is more confidential than that stored on CD-ROMs. On the other hand, they make security copying easier, which is something that is too often neglected on home PCs.

Nearly 80 per cent of home broadband connections are protected by some kind of firewall. About two in three home PCs have anti-virus software and about the same number receive regular updates for their Windows operating system. Spam e-mail is a problem only for a small minority of e-mail users.

By international comparison, Finnish households have managed their information security moderately well, but are not among the best. However, this assessment was made on the basis of information for 2002, and the situation may have improved since.

About 10 per cent of Finnish Internet users have used a credit card to pay on-line. There have been hardly any reported cases of fraud.

If experiences with the security of on-line banking are used as a yardstick for other confidential services, it is clear that the latter still have some way to go. A considerable proportion of Finns are suspicious of using a credit card on-line. Registration errors had been encountered by about one in ten Finns, which does not reflect well on the confidentiality of registers. It may also represent a certain risk to people's legal safeguards, because decision-making by public authorities based on the combining of registers could be on the increase.

The information security level of Finnish businesses is among the best in the European Union.

Government Resolution on the National Information Security Strategy, 4 September 2003



Background

The information society is based on new technology, new procedures and new expertise, the use of which will improve the welfare of citizens, change practices of interaction and social participation, and promote equality and democracy. They will also improve the productivity and competitiveness of companies and open up new markets and business opportunities. For public administration, the information society enables reform of procedures, improvement of client service and conservation of resources.

To exploit the opportunities and eliminate the threats posed by the information society, all actors must have confidence in the course of development. The confidence of citizens and companies in the information society can be increased in particular through improvements in information security and privacy protection. "Information security" refers to protection of information, services, systems and telecommunications in whatever form. Information security involves features of technical security, behaviour of individuals, procedures of organizations and social conditions.

Threats to information security include breaches of personal privacy, spam e-mail, industrial espionage, pirate copying, computer viruses, network terrorism and electronic warfare. Any of these can spread worldwide in an instant through information networks. But information security also presents opportunities. Properly implemented, it increases an individual's freedom of action, creates new business opportunities and reduces the costs of running a business and of interaction everywhere in society.

The National Information Security Strategy is an important part of the Government's information society policy. Its purpose is to combat threats to information security and to exploit related

potential under normal and exceptional circumstances. The Strategy provides a common platform for the information security efforts of the Government, businesses, organizations and individual citizens. However, the Strategy does not affect the existing division of responsibility in information security or existing organizational structures.

Strategic objectives

The National Information Security Strategy will help Finland become a safer information society.

Objectives of the strategy are to:

- 1. promote national and international information security cooperation;**
- 2. promote national competitiveness and the operating potential of Finnish information and communications operators;**
- 3. improve information security risk management;**
- 4. safeguard fundamental rights and protect the nation's knowledge capital; and**
- 5. increase information security awareness and competence.**

The strategic objectives and the practical measures related to them are discussed below in more detail. They are not presented in order of priority.

Arrangements for implementation

In a true information society, new information, expertise, technology and practices extend to all areas of life. Information security is an essential component of an information society and must likewise extend to all areas of life. This means that closer cooperation between all actors is needed. The National Information Security Strategy lays the foundation for improved cooperation, guiding information security efforts towards shared goals and promoting joint planning and implementation of information security projects and related exchange of information.

The Government has the overall responsibility for the National Information Security Strategy and oversees its implementation and updates it as needed. The Ministry of Transport and Communications appoints the National Information Security Advisory Board, which has the task of supporting the

harmonization of measures required in the implementation of this Strategy and monitoring its implementation. The Board reports annually to the Government on the implementation of the Strategy and on the need for updating it. The Board provides a broad-based forum for improving cooperation between various actors and organizations in information security issues.

To enhance implementation of the Strategy, the Board may set up working groups focusing on special issues or specific sectors.

1. Promotion of national and international information security cooperation

The production and use of knowledge with the aid of new information and communication technologies, unlimited by geographical distance, is a major force underlying globalization. The security implications of these new opportunities constitute a great challenge for authorities, companies, citizens and other actors.

The purpose of the National Information Security Strategy is to influence the creation of standards, policy guidelines and cooperation forums for promoting information security and to ensure that the division of responsibilities between the various actors in the field of information security is clear. To this end, the following measures will be implemented.





Project Chair

Juhapekka Ristola

Secretary General
Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28348
Mobile +358 400 788 530
firstname.lastname@mintc.fi

Secretariat

Secretariat of the National
Information Security Advisory Board

1.1. National Information Security Advisory Board

The National Information Security Advisory Board was set up by the Minister of Transport and Communications and given the task of supporting the coordination of measures required for implementing the National Information Security Strategy, monitoring implementation of the Strategy and presenting the Government with proposals for updating the Strategy.

The Board has met five times. Each meeting has included a discussion of the current information security situation in Finland and the status of different projects, and the issuing of instructions for further work and for the necessary reporting. Almost two hundred Finnish authorities, companies and other actors are participating in the work of the Board or the work of the working groups for the Board's various projects.

The members of the Advisory Board and the Board's views on progress made so far are presented at the start of this report.



The Advisory Board's report to the Government entitled "Creating a Safer Information Society" was handed over to Minister of Transport and Communications Leena Luhtanen on 14 December 2004. The report was presented by Board Chairman Harri Pursiainen.





Project Chair

Mari Herranen

Senior Officer
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28305
Mobile +358 40 720 1693
firstname.lastname@mintc.fi

Secretariat

Sanna Helopuro

Ministry of Transport and
Communications

Martin Andersson

Finnish Communications Regulatory
Authority (FICORA)

Severi Keinälä

Confederation of Finnish Industries
(EK)

Maria Lavonen

SSH Communications Security
Corporation

Tiina Nurmi

National Technology Agency
of Finland

Miina Ojajärvi

Consumer Agency

1.2. International cooperation

Aims and background

The aim of this project is to ensure that Finland's international cooperation in information security issues proceeds smoothly and flexibly. This can be achieved by using the most appropriate channels for active preparation of legislation and standards and for other information security cooperation in the European Union, such as within the European Network and Information Security Agency (ENISA), as well as in other international organizations (e.g. OECD) and business cooperation forums.

Finnish representatives from the information security sector regularly attend various different international forums. Resources are limited, which means that some participants (often the same few people) have to attend a number of different working groups. They are not always fully aware of the means available to other authorities, the measures that have been carried out and the existing legislation. In meetings discussing information security, the participants are not always able to supply information about the actions of the country's other authorities. In addition, the participation of representatives is not always coordinated (unclear who is participating and in which forum and meeting), or then the coordination occurs through personal networks. What's more, sufficiently thorough discussions on the matters at hand are generally not undertaken at all. Finland currently has no cooperation forum that brings together the different actors in the sector to discuss these issues.

The project working group was set up by the National Information Security Advisory Board for the purpose of reviewing the international cooperation needs in the sector. The working group has a diverse range of participants from both the public and private sectors. The aim of the project is to try and improve the level of cooperation between the Finnish participants in international forums on information security issues. A further aim is to clarify who should attend and who should actively participate in which particular information security forums (who, where and what).

The working group has begun a survey to determine details of the international cooperation and interaction on information security that Finland is currently engaged in and to examine the particular needs of the participants in regard to the demands placed on them. The survey will also look at people's experiences of the importance of participation and their views on how international cooperation is managed. It may also examine how the necessary information for contributing in the different forums can be accessed and how the Finnish participants at international forums can be easily contacted. The survey will also investigate the structure and coverage of the current cooperation network, the roles of the different parties in international cooperation, the views of those in the information security sector on the need for contributing internationally and the experiences of international cooperation. Problems and challenges involved in international cooperation will also be identified.

The intention is that the project will continue to promote and activate international cooperation in information security matters. More effective international cooperation on information security is in everyone's interests. The aim is to prepare a list of contact details of all those participating in international information security forums. The list will be posted on a convenient public website for anyone to access.

Situation in 2004 and progress in 2005

Based on the survey information obtained, the working group will evaluate the situation and the need for further development and make proposals to the Advisory Board. One part of the survey already started is the drafting of a list of contact details of those people participating in the

The survey should include details of how the information needed to contribute in different forums can be obtained, who are the relevant contacts and how people can be conveniently contacted in international forums.

international forums on information security. Additional members from both the public and the private sector have also been invited to join the working group.

The working group's programme of work in 2005 will be based on the 2004 survey and on the proposed measures submitted to the Board. The principle objective set in 2004, namely to advance the international cooperation on information security undertaken by Finns in order that it can proceed smoothly and flexibly, will continue to be the aim of the working group. The survey carried out in the first phase of the project was funded by the Ministry of Transport and Communications. A sum of EUR 20,000 was allocated for the project in 2004, and is again allocated for 2005, from the research and development funds reserved for implementing the National Information Security Strategy.

Impact and modifications

The idea of the project is to promote and activate international cooperation in information security matters. The project has a direct impact on other projects, in that other projects will, for example, benefit from the list of contact details and the survey made by the working group. Improved international cooperation in information security is to everyone's benefit. The aim is that the survey entitled *The scope for contributing to international cooperation in the information security sector* should include details of how the information needed to contribute in different forums can be obtained, who are the relevant contacts and how people can be conveniently contacted in international forums.

The preliminary outline proposals given here are presented to the Advisory Board by the working group. It can clearly be seen that there is a need for a common discussion forum. Consequently, consideration should be given to the creation of a framework for regular and well-organized opportunities to exchange ideas (some kind of joint information exchange forum), where concrete issues could be discussed covering such matters as who should participate in which international forum, Finland's position on various issues, and other topical matters.



Project Chair

Tapio Virkkunen

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28620
Mobile +358 50 369 7610
firstname.lastname@mintc.fi

Secretariat

Tero Kuitunen

Ministry of Trade and Industry

1.3. The importance of trust and information security in the New Economy

Aims and background

The aim of this project is to produce new information on the financial and economic importance of information security and trust in the corporate sector and the national economy in general. The project will allow answers to be sought especially to the question of how significant trust and confidence have become in the changeover to a network economy.

The launch of the project was partly on the initiative of the OECD and it was to be implemented as part of the OECD's Economics of Trust project. However, the OECD has had to withdraw from the project for reasons of its own. The project's implementation is now the responsibility of the Ministry of Transport and Communications and the Ministry of Trade and Industry.

Situation in 2004 and progress in 2005

The project has been carried out in two parts:

A study was carried out entitled *Trust in the New Economy – The Case of Finnish Banks*, which assessed the importance of trust and information security in business, using the Finnish banking sector as an example. The study was commissioned from LTT Research Ltd and the study report was published in spring 2004 (report 17/2004 (in English), <http://www.mintc.fi/julkaisujasarja>).

A *Competitiveness and Trust* seminar was held on 29 September 2004. It put together an overview of the importance of information security and trust within the national economy and the corporate sector from the viewpoint of companies, researchers and the authorities. The seminar was attended by more than 100 experts.

The study and the seminar have demonstrated that trust becomes more important when companies start to adopt networking methods that utilize information and communication technologies. This is usually what happens at critical stages in development. Information security is a key factor in this, as it allows users to be sure about the reliability of the basic infrastructure for their new working methods.

In introducing electronic services, the banks have successfully taken advantage of the established institutional confidence in their operations. In a network economy the banks also have a broader significance, as they "lend out" some of this trustworthiness to others by participating in business transactions as a trusted third party. The electronic payment buttons in e-commerce websites are a good example of this. The status of the banks as a source of trust within the network economy is likely to continue growing in the future.

With the spread of electronic services and networked operating methods, information security and trust are becoming a requirement for successful business operations. Paying attention to these as part of the forward planning of services and operating models saves money and brings a competitive advantage. The challenge for the authorities is to develop the operating environment in such a way that it encourages this without imposing excessive requirements or causing unwarranted additional costs.

Impact and modifications

The project has highlighted the economic and financial aspects of information security. This focus on the non-technical perspective is closely related to the Strategy projects which aim to enhance competitiveness, competence and awareness.



Project Chair

Kaarlo Korvola

Head of Information Management
Ministry of the Interior
PO Box 26, 00023 Government
Finland
Tel. +358 9 160 42796
Mobile +358 40 561 1649
firstname.lastname@sm.intermin.fi

Secretariat

Tapio Virkkunen

Project Vice Chair
Ministry of Transport and
Communications

Keith Bonnici

National Technology Agency
of Finland

Ari Hyppönen

F-Secure Corporation

Kari Lehtinen

Elisa Corporation

Terttu Mellin

Ministry of Finance

Pentti Saastamoinen

Finnish Information Processing
Association

Markku Suvanen

Ministry of Education

Teemupekka Virtanen

Helsinki University of Technology

1.4. Operating conditions needed for the different actors at national level

Aims and background

The aim of this project is to assess the achievements of the National Information Security Strategy at the mid-point of its implementation period, in spring 2005, by evaluating the plans and results of the other project working groups. The assessment will also look at the prospects of the main actors achieving the aims of the Strategy and the opportunities for implementing the other project working groups' most important development proposals during the remainder of the implementation period up to spring 2007.

The project will, as necessary, also provide recommendations on developing the content of the Strategy and on the necessary additional resources and cooperation with other information security forums or actors. A monitoring method will be established as the basis for the work and basic indicators will be created with the purpose of assessing the impact of the Strategy and its principal measures. In compiling the basic data required for this, use will be made of the Statistics Finland study of Finnish and foreign statistics and indicators on information security. Further development and adjustment of these indicators will need to be made separately within each of the other projects concerned.

This project will provide the Advisory Board with an objective interim assessment of progress with the Strategy and the operating conditions needed for the different actors to achieve their objectives. The project group's work will be concluded upon the handover of its report to the Advisory Board in spring 2005.

Situation in 2004 and progress in 2005

In cooperation with the Secretary General for the National Information Security Advisory Board, the working group's brief and its composition have been significantly altered and the group enlarged. In broadening the scope of the project, the wishes of the Advisory Board expressed after the setting up have also been taken into account in regard to matters such as the development of information security indicators. The project name was also modified to correspond with the new content.

The group's evaluation tasks and formulation of proposals will be carried out through cooperation between the working group members and consultants from the firm that wins the tender. This will make use of material and interview data collected from all the other project working groups.

The working group prepared an open tender invitation to find consultants for the work. The tender invitation was sent out to suppliers on 24 September 2004 in the name of the Ministry of the Interior. Tenders were received from five consulting service suppliers. Following comparison of the tenders received, the tender was awarded to Jaakko Pöyry Infra JP-Epstar. The consultants named for the work are Jouni Paju and Joni Tefke. The contract was signed on behalf of the Ministry of the Interior, but the costs are being funded not only by the Ministry of the Interior but also the Ministry of Transport and Communications and the Ministry of Finance.

The consultancy work will begin immediately after the contract is signed and in accordance with the project plan appended to the contract. The report is due to be ready in May 2005. The work will be based on a study of existing statistics and indicators carried out by Statistics Finland on behalf of the Ministry of Transport and Communications, and on additional material gathered by the consultants from different sources and from all project groups.

Impact and modifications

The project will evaluate the work and actions of all other project working groups and the impact of these, and will present proposals for their possible future development to the Advisory Board for its consideration. This project will therefore support all the other projects and provide ideas and proposals for the consideration of the Board in regard to guidance on further work and possibly also expanding certain projects.

2. Promotion of national competitiveness and the operating potential of Finnish information and communications operators

Information and knowledge will become ever more valuable assets in a global market that relies on the production and use of information. The National Information Security Strategy will help make sure that information is openly accessible and safe to use in Finland. This will provide new business opportunities and a stable operating environment for companies producing, utilizing and securing information. This, in turn, will improve Finland's competitiveness and produce resources for other areas of development in society.

By developing the business operating conditions for information security companies, national competitiveness will be enhanced and the availability of new and diverse information security services improved.

To this end, the following measures will be implemented.





Project Chair

Päivi Antikainen

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28460
Mobile +358 40 776 7687
firstname.lastname@mintc.fi

2.1. Programme on trust and information security in electronic services

Aims and background

At the end of 2003, the Ministry of Transport and Communications commissioned a preliminary study on the potential for having an information security R&D programme to promote the competitiveness and operating conditions of Finnish ICT companies.

The preliminary study was carried out by inviting the views of ICT company management and personnel working in specialized information security tasks. The preliminary study concluded by proposing the launch of this programme.

Among the other conclusions of the preliminary study, it was stated that this programme should not be thought of exclusively as a programme dealing with information security companies, because information security must be treated broadly as an issue affecting many different sectors. The scope of the programme should in fact cover all the different actors in product and service development within the mobile communications, Internet and digital TV sectors. A key conclusion of the preliminary study was that the programme should concentrate on developing convergence-related aspects of information security and formulating views on future information security risks and of the possible solutions for them.

The preparation of the programme was begun in late spring 2004 on the basis of the preliminary study findings. The preparatory work has included interviews with experts, business development managers and senior management of Finnish and non-Finnish ICT companies operating in Finland.

Discussions during programme preparation have indicated a more favourable attitude towards developing information security through practical services and user contexts than as a separate entity (e.g. development of individual technical solutions and applications). At the national level, it is felt that the greatest need is for formulating views on the future role of information security in different sectors and its impact on future product and service development. There is a need for information and viewpoints on the information security challenges and threats and on the type of matters to prepare for in the future. As a basis for this work it is also necessary to have a view on the type of user contexts for future electronic transactions and services in different sectors. Based on the discussions during the preparatory work, there is interest in cooperating both at the general level and especially in the form of concrete commercial projects.

Situation in 2004 and progress in 2005

Preparation of the programme was begun in late spring 2004 on the basis of the preliminary study findings. The aim of the preparatory work has been to define more precisely the sector covered and the content, objectives and approach of the programme. Besides the Ministry of Transport and Communications, the other programme participants have included the consultancy firm EERA Finland Oy. The work has included interviews with experts, business development managers and senior management of Finnish and non-Finnish ICT companies operating in Finland.

The two-year programme will begin at the start of 2005. The Ministry of Transport and Communications' budget for the programme is EUR 300,000–EUR 400,000 per year. The programme has been given the provisional title of *Programme on trust and information security in electronic services*. The content and practical implementation will be reviewed at the launch stage, when the participants and the companies interviewed at the preparatory stage will also have the opportunity to influence the form of the programme.

Digital convergence will boost product and service development and generate new issues for information security management.

The ultimate objective of the programme created at the preparatory stage is to establish the right conditions for the development of secure electronic services and for the creation of new commercial products and services. The focus will be on developing the competitiveness of Finnish ICT companies and improving their operating conditions.

The aim of the programme is to promote information security in on-line public and commercial services, on-line entertainment services and other useful services. It is also expected that the programme will lead to improvements in security in on-line public services and will stimulate product and service development in information security companies. For companies engaged in developing information security and for other actors, the programme will provide a means for applying information security solutions in practical projects.

The programme will examine information security particularly from the viewpoint of convergence in terminal equipment, networks and services. Digital convergence will boost product and service development and generate new issues for information security management. Instead of examining information security in individual technologies or communication channels, the programme aims to create a view of the future regarding the combined effect of the widespread adoption of digitalization and IP technology.

The idea is to use this knowledge to benefit product development of existing and above all future electronic service products. The programme will examine the development of electronic services in various user contexts. The focus may therefore be on, for example, future entertainment or work environments, health care, banking services or retail sales. The programme will be used to determine the information security requirements associated with convergence in the electronic services in these user environments and how they should be taken into account in product and service development and in related processes. In addition, the programme will include the launch of commercial pilot projects in which these product development solutions and operating models will be tested and developed.

In the longer run, the programme should also raise the level of consumer confidence in the use of electronic services in terms of information security issues and, by developing an innovative environment, should improve the competitiveness of Finnish companies. The programme aims to promote networking between companies and to develop a proactive approach in product and service development. In addition, the aim is to improve global awareness of the frontrunner status of Finnish companies and Finnish society in information security and to promote the development of national and European regulations and legislation.

The Ministry of Transport and Communications will set up a working group for the programme at the start of 2005, which will have the job of directing the programme work and setting targets for it. The group will also approve the programme indicators to be used for measuring progress towards the programme targets.



Project Chair

Jaana Lappi

Senior Adviser
 Ministry of Trade and Industry
 PO Box 32, 00023 Government
 Finland
 Tel. +358 9 1606 2658
 Mobile +358 50 308 8143
 firstname.lastname@ktm.fi

Secretariat

Joni Halmelahti

Federation of Finnish Enterprises

Marja Heinonen

Ministry of Transport and
 Communications

Kari Keskitalo

Ministry of Trade and Industry

Tuija Kyrölä

Helsinki Chamber of Commerce

Terttu Mellin

Ministry of Finance

Petri Puhakainen

Laurea Polytechnic

Helvi Salminen

Setec Oy

Timo Simell

Finnish Information Society
 Development Centre (TIEKE)

Kalevi Tiihonen

Confederation of Finnish Industries
 (EK)

2.2. Corporate information security awareness

Aims and background

Understanding of the responsibility for information security in society has not advanced in the way envisaged. The responsibility for ensuring information security rests with all actors in society: as much with the public and private interests in charge of the infrastructure as with the businesses and private individuals who use the networks and information systems. Information security awareness and an understanding of the impact of the risks are particularly essential for companies whose operational continuity, development and competitiveness all rely on functioning information systems. The development of electronic commerce, the increasing amount of on-line business, and especially the networking of business activities and the challenges that this brings, have encouraged debate on information security questions and focused attention on the need for practical measures.

Developing information security and managing information risks is a demanding task for any company. The increasing complexity of information systems and applications and the rapid expansion of capacity impose demands on competence and resources. Small enterprises, in particular, are in a weaker position.

Very little information has so far been available in Finland about the level of corporate information security awareness. A number of separate studies have demonstrated that concern over the extent and quality of information security has indeed increased, but practical measures are some way behind. The dominant view is that information security is simply a technical matter that can be managed with technology and the right hardware and software. However, as information users and computer users, people themselves are in a key position, and improvements in information security awareness are dependent on the motivation of users. The role of corporate management is especially important.

The working group's main aim is to increase information security awareness and action among businesses and especially small and medium-sized enterprises (SMEs). The goal is that corporate management and personnel should be aware of the importance of information security and the potential risks, their own role in eliminating the risks, and the positive contribution of information security to the business. In addition, the aim is to promote awareness of the types of measures that can be taken to enhance information security.

The aim of the project is to promote an appropriate level of information security awareness in companies and other organizations. This involves the following elements:

- a) gathering information on the actors that promote information security awareness and on the measures taken;
- b) defining the targeted level of corporate information security awareness;
- c) drawing up recommendations on the actions for coordinating existing projects/measures designed to promote information security awareness; and
- d) drawing up recommendations regarding any new projects/measures that may be needed.

Developing and improving corporate information security awareness is a process that begins by ensuring that the management and personnel are aware of its importance. By being aware of the importance of the issue, employees will be motivated to act accordingly. The working group has so far concentrated on acquiring suitable information security awareness training programmes and making recommendations on their use to SMEs.

The aim of the seminars is to provide useful information on the importance of information security for businesses and to give practical advice on improving corporate information security.

It is essential that these information security awareness programmes, projects and measures are incorporated as effectively as possible into practical everyday operations. This is a challenging communication and dissemination task for all the parties involved.

Meetings have formed an essential part of the project, and the costs of these meetings have been met by the host in each case. The working groups have also made extensive use of e-mail in their work. The participants have not received any reimbursements or fees for their work and each of the participating bodies has been responsible for meeting its own costs.

Situation in 2004 and progress in 2005

The project working group began its work in April 2004 by gathering information on the actors involved in promoting corporate information security awareness and on the measures taken, and by defining the existing and targeted state of corporate information security awareness. Using this information, the working group will make decisions and issue recommendations for improving the awareness. The working group will also formulate and present a concept/tool that companies can use in planning and implementing their information security awareness training programmes. The aforementioned elements of the project will form a key part of the project report, *Improving corporate information security awareness*, which will be completed in December 2004.

The working group will continue its work in 2005. It aims to support and coordinate measures to increase corporate information security awareness and to cooperate closely with other public and private organizations implementing the National Information Security Strategy. Owing to the large number of companies being targeted, the information security messages and the measures to increase corporate awareness will be modified accordingly during 2005.

The Ministry of Trade and Industry is planning to introduce a series of information security awareness seminars for SMEs in ten Employment and Economic Development Centres in 2005 in conjunction with the Centres and other bodies involved in promoting corporate information security awareness. The aim of the seminars is to provide useful information on the importance of information security for businesses and to give practical advice on improving corporate information security.

It is proposed that the Advisory Board conduct an impact assessment of the recommendations and measures to be introduced.

Impact and modifications

Appropriate awareness of information security will assist in the development of the information society and also enhance corporate competitiveness. Information security is a tool for increasing corporate confidence in the potential of information and communication technologies. Companies making extensive use of ICT will be able to gain a competitive advantage and improve their efficiency.

The aim is that the working group's report will set the main guidelines for the action to promote corporate information security awareness.



Project Chair

Keith Bonnici

Senior Technology Adviser
National Technology Agency
of Finland
PO Box 69, 00101 Helsinki
Finland
Tel. +358 10 521 5777
Mobile +358 50 5577 777
firstname.lastname@tekes.fi

Secretariat

Mikko-Pekka Hanski

Idean Research Ltd.

Hannu H. Kari

Helsinki University of Technology

Petri Lillberg

SSH Communications Security
Corporation

Kari Oksanen

Nordea Bank Finland Ltd

Pirkka Palomäki

F-Secure Corporation

Juha Perttula

Ministry of Transport and
Communications

2.3. Convenient and compatible products and innovative areas for development

Aims and background

In this project, companies and research institutions are encouraged to bring new information security products to market, develop protection and identification methods that are convenient and compatible with other products, and disseminate the best practices to other actors.

In addition, the project supports the use of appropriate information society and technology policies to encourage innovative ideas for information security development, the formation of corporate and organizational competence networks, and partnership programmes between public and private-sector actors.

The main objective of the project is to promote the international competitiveness of existing information security companies by supporting their R&D work and business skills. The aim of the National Technology Agency's SWENG programme, for example, is to improve software production and the quality of software products and processes. A further aim is to create new internationally competitive information security companies in Finland. An indirect aim is to promote the introduction of information-secure electronic services in Finnish companies, universities and other higher education establishments, research institutions and other public organizations.

These kinds of corporate projects have included the following: *Secured and remotely managed WLAN solution* (Vioteq Ltd), the EUREKA joint project (Comptel Corporation, SSH Communications Security Corporation, SiltaNet Ltd, Ubisecure Oy, and others), and *Using software-based PKI primarily in mobile banking services and electronic transaction services* (Meridea Financial Software Ltd). On the research side, there are also several high-level projects, including: *Authentication and authorization of short-range radio frequency technologies* (Information Technology Department of Lappeenranta University of Technology), *Security topics and mobility management in hierarchical ad hoc networks* (Laboratory of Information Processing Science at Helsinki University of Technology), and *Secure self-organized mobile networks* (VTT Electronics).

Other active measures include the Finpro eGovernment programme funded by the National Technology Agency. The programme involved the participation of eight SMEs during 2004. The companies made use of National Technology Agency funding to finance the project. The principal aim of the project is to promote the internationalization of information-secure Finnish eGovernment software products and companies. In the eGovernment programme, companies have commissioned or acquired various market surveys, legal analyses and business analyses, and have met potential partners and distributors individually in different European countries. The National Technology Agency activates Finnish companies to participate in EU projects and has organized networking between Finnish and Italian, Israeli and other companies.

Various other Agency-funded corporate projects are also in progress but have not been made public. Some of the corporate and research projects are multi-annual and will continue in 2005. Under its normal funding criteria the National Technology Agency is also funding corporate R&D information security projects and similar projects for universities, other higher education establishments and research institutions. Applications for corporate projects are considered throughout the year. The extent and form of funding is determined separately for each project. The project period is 2004–2006.

Information security matters should not be considered merely in terms of separate software packages or functions but as a natural part of the company's business and product development, whatever the sector of operation.

Situation in 2004 and progress in 2005

More detailed inspection and analysis has revealed that various Finnish organizations already have information on the current level of information security in Finnish SMEs throughout the country. The results are very encouraging: 95 per cent of companies in the Uusimaa region are using an anti-virus software package or service and 75 per cent are using a firewall. It is also apparent that there are numerous services and certificates on the market that allow companies to assess and define their level of information security.

Based on the above-mentioned studies and information, the project group came to the conclusion that there is already sufficient basic information on the market regarding the existing level of corporate information security. Furthermore, the objectives of many of the other projects include determination of the existing information security level of Finnish companies. To avoid duplication of work, the group decided not to pursue this any further.

A new objective for the group is to examine the scope for integrating information security and related matters more firmly into the National Technology Agency's existing and future technology programmes. Information security matters should not be considered merely in terms of separate software packages or functions but as a natural part of the company's business and product development, whatever the sector of operation.

The project group is actively following developments in information security issues both in Finland and abroad and aims to disseminate this information to the National Technology Agency's customer companies and other enterprises and research institutions.

Impact and modifications

With the aid of National Technology Agency funding and support, many Finnish companies and research organizations in the information security sector have successfully improved their international competitiveness by developing new, innovative and diverse information security products and services.

The National Technology Agency's new start-up loans (capital loans for setting up technology companies) allow it to support the creation and development of new companies in the sector more effectively than before. Funding will continue in 2005 through the normal Agency criteria.



Project Chair

Terttu Mellin

Senior Officer
Ministry of Finance
PO Box 28, 00023 Government
Finland
Tel. +358 9 160 33214
Mobile +358 40 820 3254
firstname.lastname@vm.fi

2.4. Harmonizing public-sector information security procedures

Aims and background

The aim is to provide public-sector actors with guidance on introducing greater harmonization in their ICT-based operating procedures, which will include consideration of information security aspects, both within the public sector and between the public and private sectors. The project is also part of the continued effort to issue guidelines on this subject for central government and partly also for local government. The existing guidelines will therefore be brought up to date and augmented. Networking has proved to be a good way of distributing information about information security and of improving procedures. The Public Management Department at the Ministry of Finance is responsible for general guidance and development on government information security. The Public Management Department's principal activities in information security guidance include issuing government guidelines on information security, arranging joint projects on information security, cooperating at national and international levels, and the diverse activities of the Steering Committee for Data Security in State Administration (VAHTI) set up by the Ministry of Finance covering all areas of information security and all branches of government.

Situation in 2004 and progress in 2005

The work of the Steering Committee for Data Security in State Administration set up by the Ministry of Finance was continued in 2004. The information security projects of the Ministry and the Steering Committee are always based on extensive cooperation within the government sector, which is focused on reconciling different views, and relevant organizations and business interests also participate where necessary. A number of Ministry and Steering Committee projects have already resulted in further improvements in the harmonization of public-sector information security procedures. Making use of the results of these projects at municipal level too has progressed, and the municipalities have also been cooperating in the preparatory work as necessary. In information security matters, the Ministry and the Steering Committee also cooperate with the Advisory Committee on Information Management in Public Administration (JUHTA), the Ministry of the Interior, the Association of Finnish Local and Regional Authorities, and municipality representatives.

The Ministry of Finance has published a plan entitled *Finnish Government information security development plan for 2004–2006*. Implementation of the plan has already begun and is being led by the Ministry. The coordination, monitoring, preparatory work and harmonization aspects are the responsibility of the Steering Committee. The wide-ranging plan includes measures for improved harmonization of public-sector information security procedures. Participants in the plan's implementation include many different government bodies, the municipal sector, the corporate sector and other organizations, as necessary. For example, about 300 people from the government sector have already been actively involved in the preparatory work for the development plan projects and in the cooperation at government level. The plan contains 28 development targets, and projects were launched in 22 of these during 2004.

The projects all include the necessary cooperation with municipal government, relevant organizations, business interests and international actors, and joint action is also arranged where needed. The plan's development targets also represent important areas of information security work for municipal government and the corporate sector. The period applying to almost all the development plan projects is to be extended to at least 2005. The wide-ranging information security guidelines issued by the Ministry of Finance have been added to and

further developed as necessary, as part of a continuous process. New guidelines were issued in 2004 on matters including results management in information security, combating malicious software, and user action on information security. Preparations are currently in progress on various matters such as guidance for handling of datasets, securing e-mail and measures to deal with information security violations and other exceptional events. The work to maintain and improve the guidelines will continue in 2005.

Development plan projects already completed or currently in progress concern the following targets outlined in the plan:

- results management in information security and quantification of results
- information security as an integral part of processes in government agencies
- combating spam e-mail
- role of ordinary users in information security
- use of certification in government e-mail traffic
- identifying users and administering user authorizations
- 24-hour information security in central government
- cooperation between government-sector organizations in international information security work
- making use of shared resources in information security work
- information security in communications networks and terminal devices
- information security in document management
- electronic surveillance and development of privacy protection
- information security in the basic infrastructure
- information security and contingency planning
- information security assessments
- joint government information security projects
- continuous development and updating of the information security guidance of the Ministry of Finance and Steering Committee for Data Security in State Administration
- information security seminars and good practice
- training in information security issues
- strengthening the work of the Steering Committee for Data Security in State Administration
- cooperation with the Information Society Programme
- maintaining anti-virus capability

Impact and modifications

The information security work of the Ministry of Finance and the Steering Committee for Data Security in State Administration and their guidelines cover all areas of information security. They include not only information system and network security but also government information security, dataset security, security of premises and privacy protection. The Ministry's guidelines on information security are of use not only in central government but also in municipal government and the corporate sector, and in international cooperation on information security. The information security guidelines are published in printed form and can also be viewed on the Ministry of Finance website at www.vm.fi/vahti. The Ministry's guidelines, the Steering Committee for Data Security in State Administration's activities and the joint information security projects have together resulted in more effective information security work of a continuous and proactive nature within the government sector. The development plan's measures already completed or in progress make use of the information security work carried out within the government sector, which is of a long-term nature, diverse and broad-based. They also improve the effectiveness of government information security work and related joint actions, and improve the development and utilization of expertise. The development plan will also enhance the efficiency with which the information security work in the government sector is used in different sectors of society, as well as cooperation between the government and other sectors.

The plan is designed to meet today's information security challenges and to anticipate future challenges, strengthen joint working and development in information security, and encourage the allocation of resources to development targets of key importance for information security. The plan also provides strong support for implementation of the objectives of the National Information Security Strategy. The plan's interpretation of information security is very broad and includes not only ICT functions and electronic data and ICT security, but also other information security viewpoints such as handling paper documents and the protection of privacy. Information security requires organizations to have sufficient investment and competence. Simply acquiring hardware and software is not enough. It is also necessary to develop personnel skills and data administration competence, to incorporate information security in service agreements and to ensure there are sufficient funds allocated to information security measures in the budgets for each branch of government and for each agency. Improving information security as set out in the plan will require parallel development of the organization's processes, working methods, training for personnel and other users, and technical solutions. The development plan will later be evaluated as a whole.

The Ministry of Finance's information security guidelines, development plan and other working models have also been presented during the course of international cooperation on information security, where they have been seen as examples of good practice in promoting a culture of information security. A need has been identified for combining this project (2.4.) and project 5.3. (*Information security awareness in public administration*). The focus areas of these projects, namely harmonization and awareness, are aspects which, in practice, are and should be promoted jointly and not separately.



Project Chair

Sanna Helopuro

(from 1 May 2004)
Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28608
Mobile +358 400 515 548
firstname.lastname@mintc.fi



Project Chair

Kirsi Miettinen

(1 January – 30 April 2004)
Special Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28305
Mobile +358 400 629 719
firstname.lastname@mintc.fi

2.5. Impact assessment of legislation

Aims and background

The threats and risks associated with different functions in society have long been managed by means of legal regulation. It is no wonder, then, that attempts to control information security threats and risks have also focused on regulation. Legislation to improve information security has been drafted on the basis of identifying and evaluating the threats and risks involved.

A significant amount of new legislation concerning information security has been enacted in recent years in Finland. Even though legal provisions may not always mention the term information security directly, there is a lot of new legislation on, for example, privacy protection, which indirectly concerns information security. Information security can in fact be seen as an integral part of several of the fundamental rights safeguarded in the Finnish Constitution.

The increase in legislation on information security and the fact that provisions on it are found in many different acts presents a challenge for the experts on information security. It also raises the question of how effective the existing information security legislation is, whether or not there is too much of it or too little, and what remains to be done.

Legal research on information security is also a relatively new field. Although information security has been taken into account in development of the regulations on personal data protection from an early stage, the subject has long been given scant attention in jurisprudence.

The aim of this project is to regularly assess the effects of the legislation and treaties concerning information security and the information society in terms of the development and use of communications services, on-line banking services, electronic identification services, electronic commerce, and on-line government services. The assessments should allow problems to be identified and therefore answers found to the questions mentioned above.

The purpose of the project is to obtain a clear and realistic picture of the legislative sphere in its entirety and to identify any deficiencies and weaknesses. To this end, the project will examine the elements of Finnish legislation and international agreements that are relevant for information security. This will provide a clear picture of the coverage of the legislation, any gaps in that coverage and any detrimental duplications.

Situation in 2004 and progress in 2005

On the basis of a separate analysis, the project working group looked at how well the legislation on information security serves companies and other organizations in issues and problems related to information security, and the extent of awareness of the legislation. The working group has not set out to determine the extent of the existing legislation on information security, because it understands that this is being done in connection with project 4.1. (*Ensuring fundamental rights*). For this reason, the working group has also closely followed the work in that project.

The aim of the working group's investigation was to obtain information from the different actors in the sector on how they view the impact of the legislation in everyday dealings with information security, i.e. what they see as the current information security problems and threats for companies and how the existing legislation has aided or hampered measures concerning information security. The work was conducted in the form of an interview survey. The Ministry of Transport and Communications has reserved a sum of EUR 25,000 for this work.

Secretariat

Hellevi Huhanantti

Population Register Centre

Antti Järvinen

Kesko Corporation

Heikki Partanen

Office of the Data
Protection Ombudsman

Olli Pitkänen

Helsinki Institute for
Information Technology HIIT

Kari Wirman

Elisa Corporation

Preliminary findings based on the survey:

- Companies were not able to identify precisely any individual “problem clauses” in the legislation that directly concerns information security.
- Companies do not feel the need for further legislation but instead desire more effective application of the existing legislation and more cooperation.
- At a general level, the legislation was felt to be unclear. The main reasons for this were an incomplete awareness of the information security provisions and interpretation problems connected with the legislation.
- Corporate awareness of the specific information security legislation varied greatly.
- Interpretation of the law generally falls to the information management director (only the biggest companies have their own lawyers).
- It was felt that privacy protection limits information security measures.

Survey indicates a desire for the following:

- cooperation forums,
- self-regulation,
- regulations and binding instructions from the authorities, and
- sharing of responsibility (e.g. extending product liability to software as well).

Following the survey, the working group will, in December 2004, draw up a report and proposals for action based on its findings and experiences.

Impact and modifications

The impact of the project will be an improved ability to identify the causes of any problems concerning the information security legislation. It should also be possible to identify the main questions related to the information security legislation, and to use the project to seek answers to these questions. This will allow a balance to be found between legislation and action on information security. Together with the project on ensuring fundamental rights, this project will produce an overview of the legal framework currently applying to the information security sector.



Project Chair

Juha Perttula

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28617
Mobile +358 400 694 419
firstname.lastname@mintc.fi

Secretariat

Heikki Ailisto

Technical Research Centre of
Finland (VTT)

Kaarlo Karvonen

Finnair Plc

Lauri Karppinen

Office of the Data Protection
Ombudsman

Tuomas Kivinen

Nordea Bank Finland Ltd

Tommi Rakshit

Ministry of the Interior

Ari Saapunki

Aldata Solution Finland Oy

Tuire Saaripuu

Population Register Centre

Helvi Salminen

Setec Oy

2.6. Information security and privacy protection in biometric identification

Aims and background

Biometric identification, i.e. identification based on a person's physical characteristics or behaviour, enables the development of new kinds of services and could therefore bring new business opportunities for service providers. Biometry looks likely to play an important role in electronic identification in many respects in the near future. Methods will be developed which are more accurate and reliable than at present and an increasing number of new applications for them will be found.

Trust is a key factor in the development, use and spread of biometry and applications and services that use biometric methods. Biometry has proved to be particularly demanding in terms of gaining user acceptance, and it seems to give rise to all kinds of suspicions, many of them unfounded. Nevertheless, there are features of biometry where the importance of information security is particularly emphasized.

Ensuring information security in identification systems is a key factor in building up trust in the methods used. Service providers and other actors using biometry are still not fully aware of all the information security aspects. They need more information about the aspects of information security that they should be taking into account in their biometry-based services and systems.

The aim of this project is to examine the information security questions and possible risks and problems concerning the use of biometric identification. The idea is to assess whether biometric identification has any characteristic features that would give cause for special attention to certain areas of information security. The assessment should also give due consideration to essential aspects of the views concerning privacy protection and other fundamental rights in relation to biometric identification.

By investigating and analysing the information security issues, the aim is to promote business opportunities for Finnish companies and the development of services that use biometric identification. The aim is also to promote diversity in the use of biometric identification. Among the different aspects of information security, the project will probably concentrate on confidentiality in particular, rather than areas such as the demands concerning usability of services.

The implementation of the project will also contribute to ensuring that issues of information security and privacy protection are taken into account sufficiently in the development of biometric identification in Finland, and that the information security risks are adequately managed.

Situation in 2004 and progress in 2005

The project implementation plan was presented to the National Information Security Advisory Board on 15 June 2004. A project working group was set up for the period 1 December 2004–31 December 2005. The initial work included a survey of the national actors in the sector.

In assembling the working group, the principle was that it should include the best experts from the public and private sectors and the research field. In addition, the views of the main actors and experts will be sought at the group's meetings as necessary. The project begins with an examination of what has been studied on the subject and also looks at the aims of other key projects. The Ministry of Transport and Communications will finance any necessary consultancy studies in the first phase of the project. R&D funds totalling EUR 30,000 have been reserved for the project in 2005.

Impact and modifications

The purpose of the project is to promote business opportunities for Finnish companies and the development of services that use biometric identification, and to combat the threats to privacy protection presented by biometric methods.

The service providers and other actors using biometry are still not sufficiently aware of all the aspects of information security, and so they have a pressing need for information on the information security aspects they should be taking into account in their biometry-based services and systems. Such information and expertise is also of key importance from the viewpoint of privacy protection, which will be highlighted in the future development of interoperable biometry-based systems, for instance by developing standards for this.

The implementation of the project will contribute to ensuring that issues of information security and privacy protection are taken into account sufficiently in the development of biometric identification in Finland, and that the information security risks are adequately managed. The project supports the 2005 priority project 3.2. (*Analysis of national information security risks*).

3. Improving information security risk management

Safe use of information is a growing challenge for all actors in society at large because the known risks are changing and new threats are emerging all the time. The purpose of the National Information Security Strategy is to encourage individual citizens, companies and other actors in society at large to identify and manage risks in an anticipatory manner.

A proper anticipatory approach will help to guarantee the best possible security and minimize security-related costs. To this end, the following measures will be implemented.





Project Chair

Juha Perttula

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28617
Mobile +358 400 694 419
firstname.lastname@mintc.fi

Secretariat

Ilkka Ahola

Sun Microsystems Oy

Kaj Arnö

MySQL AB

Kimmo Bergius

Microsoft Oy

Kauto Huopio

Finnish Communications Regulatory
Authority (FICORA)

Kalevi Hyytiä

The Finnish Defence Forces

Juha Härkönen

Fortum Corporation

Urpo Kaila

Finnish IT Center for Science (CSC)

Erka Koivunen

Elisa Corporation

Sami Lehtonen

Technical Research Centre of
Finland (VTT)

Perttu Luhtakanta

The Finnish Defence Forces

Usko Moilanen

National Bureau of Investigation

Simo Tanner

Association of Finnish Local and
Regional Authorities

Stefan Zilliacus

Symantec Finland

3.1. Assessing and more effectively combating information security risks

Aims and background

The costs and problems arising from information security risks are on the increase in all areas of society. Thus, more needs to be done to combat their negative impacts. However, there is no clear view of how information security risks are evolving, what long-term action is required, or how the corrective measures should be prioritized. For example, harmful communications and malicious software are threatening to spread to hitherto unaffected operating environments.

Many actors still have an unfocused and unsystematic approach to risk assessment methods. An actor wanting to know more about the matter can of course draw on a wide variety of national and particularly international sources covering different aspects of information security risks. Finding the information that is relevant and useful to the actor's own organization may, however, be much more time-consuming. These problems are particularly difficult for SMEs and other small-scale actors, which need to know more about information security risks relevant to their operations. The long-term objective is to reduce the harmful impacts of information security risks. The aim of the project is to produce a long-term assessment of the most significant information security risks and risk trends and to present proposals for long-term risk prevention on a regular basis.

Another objective is to promote appropriate and workable risk-assessment practices and methods. The aim is to identify factors and operating approaches that can be used directly or indirectly to help put risk assessment on a more systematic and comprehensive footing. This should lead to a long-term reduction in the negative impacts of the most serious information security risks and ensure maximum usability and security of the network environment despite any information security threats.

Situation in 2004 and progress in 2005

The working group presented the information security risk assessment implementation plan to the National Information Security Advisory Board on 16 March 2004 and the project was launched in April. The project aims include assessing the most serious shortcomings in the existing risk assessment activities and determining the most common effective and well-tried means for improving information security. At the same time, the aim is to find and produce workable and suitable approaches and risk assessment methods for future project work.

The project will also involve drawing up a checklist that can be used for assessing information security in the processing of identification and location data by corporate or association subscribers in the SME sector, and in the implementation of the selected methods. The working group decided to focus on the needs of small-scale actors, as their systems and procedures are probably in the greatest need of information security improvements.

Under the new Act on the Protection of Privacy in Electronic Communications (516/2004), corporate or association subscribers must maintain information security when processing their users' identification and location data. The term "corporate or association subscriber" covers a large number of small actors that, because of insufficient resources, often have a haphazard approach to information security. A corporate or association subscriber means a company or an organization that subscribes to communication or value-added services and which processes users' confidential messages, identification or location data in its communications network. The definition applies to companies, associations, educational institutions, government agencies, businesses, housing companies, individual computer users, public sector bodies, etc. that have access to equipment that can store users' identification data or communications, such as a switchboard or an e-mail server.

It is important to remember that, as information security covers all aspects of ICT, its application to any part of a corporate or association subscriber's operations must be preceded by comprehensive evaluation and design of the subscriber's procedures and systems.

It is important to remember that, as information security covers all aspects of ICT, its application to any part of a corporate or association subscriber's operations must be preceded by comprehensive evaluation and design of the subscriber's procedures and systems. Information security can only be properly maintained if all the systems, networks, servers, terminals and other equipment, software and procedures that are used for processing identification and location data meet the necessary requirements. For SMEs, managing the information security aspects of identification and location data processing may also have wider information security implications.

The working group conducted a vulnerability analysis of identification and location data processing by corporate and association subscribers. The analysis began with a brainstorming session aimed at charting and identifying all information security threats that can affect the processing of identification and location data by a corporate or association subscriber. The information security threats identified were grouped as follows: dataset security, software security, operating security, communications security and hardware security. The classification is in accordance with the division used in the Act on the Protection of Privacy in Electronic Communications.

The vulnerability analysis produced a comprehensive list of threats which was then modified, subdivided and reviewed, leaving only those threats that are relevant to the processing of identification and location data. Further revisions were then made using the seriousness of threats as a basis. The likelihood of the threats, the seriousness of the consequences, level of technological development, and costs were used as criteria.

The checklist is not exhaustive and should not be considered an interpretation of the contents of the information security obligation referred to in above. The aim was to produce a checklist of the most important matters that a corporate or association subscriber in the SME sector should focus on when assessing the information security risks involved in the processing of identification and location data. This part of the work should be completed by the end of 2004.

As for the problems generated by malicious software, the working group will examine how these problems can best be reduced. The viewpoints of all actors for whom the matter is relevant and who can contribute to solutions to the problem will be taken into account, and the measures will be prepared on this basis.

A comprehensive report and information package on spam e-mail will be produced as part of the project. It will also cover the existing methods available for dealing with the harmful impacts of spam. The aim is to produce an information package that is comprehensive, easy-to-use and balanced and that would be primarily in a form suitable for on-line use. The material is intended for such groups as consumers, companies, direct marketing establishments, communications businesses and public administration.

Some of the topics to be covered by the material:

- Content of the legal provisions in force and any codes of conduct
- Regarding the legal provisions, the focus will be on national and EU-level legislation, but the main points of spam e-mail provisions in regions such as Asia and the United States will also be included
- Easy-to-use information for ensuring that the existing codes of conduct and the provisions of the new Act on the Protection of Privacy in Electronic Communications and the rights contained in them are widely understood
- Practical information about marketing practices that are based on consent, for example about what type of personal data may be collected
- Information about existing codes of conduct applied by businesses, appeal procedures, labels (such as reliability labels) and certification systems
- An overview of the achievements of the most important international forums dealing with the problem of spam e-mail, and the regulations, recommendations and instructions each forum is expected to present in the near future
- Information that is as comprehensive as possible on how the phenomenon manifests itself, and its negative impacts
- A rough overview of the links between spam e-mail and other phenomena, such as different types of vulnerability
- Information on the scale of the spam e-mail problem
- Information about spam e-mail fraud and fraudulent marketing practices
- Information about punishments received by spammers and the legal proceedings involved
- Answers to frequently asked questions
- Methods for combating the harmful impacts, such as prevention, technical solutions, legal instruments and international cooperation
- When methods are assessed, consideration will be given to the roles of the senders, transmitters and recipients of spam e-mail, the measures available to supervisory authorities and any action by lawmakers
- If possible, the methods and measures should be prioritized and a timetable for them prepared
- Practical information for companies on how they can protect their e-mail servers and equipment so that they cannot be used as spam e-mail servers
- Practical information for consumers on how to combat spam e-mail (such as address munging and information about on-line behaviour)
- Practical information for consumers on products and services that are available for combating spam e-mail (such as filtering and information security functions)
- Information about any practical measures for dealing with spam e-mail, such as appeal procedures and any alternative dispute resolution procedures that may be developed
- Future prospects, any new combating methods planned and other relevant information

The work on spam e-mail was launched in October 2004 and is to be completed by the end of February 2005. The proposals for measures to combat the problem form a separate entity and should be ready by the end of 2004. A separate steering group has been set up to manage the progress and content of anti-spam measures. The steering group members are Urpo Kaila (Finnish IT Center for Science, CSC), Sami Lehtonen (VTT), Stefan Zilliacus (Symantec) and Juha Perttula (Ministry of Transport and Communications).

The aim for 2004 is to find efficient and workable methods for the information security risk assessment work and to ensure its continuity. In 2005, the focus will be on assessing the main long-term trends in information security risks and the measures for managing these risks. The necessary studies commissioned from consultants will be funded by the Ministry of Transport and Communications. In 2004, a total of EUR 21,000 in R&D funds was spent on the project, and EUR 30,000 has been budgeted for the project in 2005.

Impact and modifications

Open information networks are becoming increasingly vulnerable to different types of information security threat. For example, worms, viruses and spam e-mail are affecting telecommunications, other communications and the usability of information systems and different services. Far from there being any relief in sight, the opposite is in fact the case. If there is a deterioration in information security in different systems, confidence and trust in the Internet and ICT in general may falter. Companies may start removing their systems from open networks, and the spread of electronic services may slow down or come to a standstill. It is only a question of time before companies and individual citizens start suffering substantial financial and operating losses as a result of information security threats.

These problems can only be tackled effectively by adopting a long-term perspective and pursuing long-term measures. Permanent solutions to all problems may never be found but more needs to be done to reduce the negative impacts. The aim of the project is to examine how to minimize the harmful effects and the cost burden to society at large.

This project supports project 3.2. (*Analysis of national information security risks*). Cooperation with the chairs of the other projects supporting project 3.2. should help to ensure that common goals are pursued and that duplication of work is avoided. As far as this project is concerned, consideration will also be given to cooperation with those projects which are aimed at increasing information security awareness. This is because the impact of this project will greatly depend on how effectively the views and proposals for measures drawn up as part of it can be disseminated to the different actors.



Project Chair

Timo Lehtimäki

Head of Information Security
Finnish Communications
Regulatory Authority (FICORA)
PO Box 313, 00181 Helsinki
Finland
Tel. +358 50 514 8286
firstname.lastname@ficora.fi

Secretariat

Jani Arnell

Finnish Communications
Regulatory Authority (FICORA)

Tuomo Hakola

Ficix

Sami Holopainen

Elisa Corporation

Sari Kajantie

National Bureau of Investigation

Veli-Pekka Kuparinen

National Emergency Supply Agency

Terttu Mellin

Ministry of Finance

Juha Perttula

Ministry of Transport and
Communications

Terho Rintanen

The Finnish Defence Forces

Mikko Viitasaari

TeliaSonera Finland Oyj

3.2. Analysis of national information security risks

Aims and background

The aim of the project is to establish a convenient system for the analysis of national information security risks which allows the analysis to be regularly updated and maintained by the Finnish Communications Regulatory Authority and made available to the principal actors in the sector.

The analysis must be kept up-to-date and provide the actors with details about information security developments and the latest threats. It must also assist customers in their decisions on how to implement information security solutions. Other aims are to help different customer segments respond to information security threats and to further the development of a culture of information security and its monitoring. An overall objective is to provide a comprehensive picture of information security and prevent any problems from arising.

Furthermore, the analysis is also intended to prevent problems from spreading by disseminating information about them – after all, many functions are highly interdependent. The aim is that the analysis will be both dynamic and static and that analysis reports will be disseminated through different channels, including the media. The information gathered will be based on the information received by the Finnish Communications Regulatory Authority (FICORA) from its partners through CERT and on information provided voluntarily. Cooperation in drawing up and disseminating the analysis work is expected to function in both normal and exceptional situations. The work of drawing up the analysis will focus on the functioning of electronic communications and the information security of communications networks. Attention will also be paid to threats to critical infrastructure.

Most of the project work has been in the form of meetings, and the costs of these meetings have been met by the host in each case. The working groups have made as much use of e-mail as possible. The participants have not received any reimbursements or fees for their work and each of the participating bodies has been responsible for meeting its own costs.

Situation in 2004 and progress in 2005

The FICORA CERT-FI group, which is the national CERT authority, has been working on an analysis of national information security risks since early 2002. It has used a variety of sources, such as the actual and attempted information security violations reported to the CERT-FI group, and public and non-public mailing lists and forums dealing with issues related to matters such as software vulnerability and malicious software. This information security risk analysis drawn up from different sources has been widely disseminated, for example as CERT-FI warnings and guidelines on the FICORA website, through mailing lists and through the teletext service of the Finnish Broadcasting Company. The CERT-FI group has also issued press releases on threats endangering the functioning of national information networks and threats affecting end users.

Drawing up of an analysis of national information security risks is one of the central objectives of the National Information Security Strategy. The aim of the working group is to create a process for establishing and disseminating analyses of national information security risks that can be used conveniently and meet the requirements of all parties. The working group has begun by examining the existing models and using them as a basis for achieving the target described in the National Information Security Strategy, i.e. the establishing of a convenient system for the analysis of national information security risks and dissemination of this information that meets the needs of all parties. The working group has studied the way FICORA

and other bodies approach the task of analysing national information security risks. FICORA has formulated, modelled and fine-tuned its own processes for building the analysis and disseminating its results and has launched an internal project with the aim of developing and strengthening the process of drawing up of a national information security risks analysis. It has also modelled a technical description of the drawing up and dissemination of an information security risk analysis. This description has been given a specific security classification and is updated on a real-time basis. A number of cooperative ventures have also been launched. A good example is the expanding cooperation between the Finnish Broadcasting Company and CERT-FI and, as part of this venture, the distribution of analysis information through various channels, and the exchange of information with partners acting as information sources. Concrete measures also include the provision of more detailed dynamic analysis information on the section of the CERT-FI website dealing with the latest on information security, and the specification and testing of technical information systems related to the analysis.

FICORA's CERT-FI group has also begun the distribution of dynamic and static analysis information, which is posted as situation updates in the CERT-FI section of the FICORA website. The updates deal with information security issues such as malicious software, its impact in Finland, spam e-mail, the number of problematic information systems and the latest developments in information security breaches and vulnerabilities. The updates cover the preceding twelve-month period, but the focus is on developments during the latest three months. An analysis of the outlook for information security during the ensuing three months is also given. A press release is issued about each situation update. In order to prepare for mobile threats, FICORA has also established a test environment for monitoring information security threats associated with the use of smart phones and for possible analysis of them. It has also started purchasing items from different operators on the Internet and through fixed IP addresses so that it can monitor how threats are evolving in the virtual space of different telecommunications companies. The necessary Internet connections are purchased through consumer and business customer interfaces. The need for an analysis of national information security risks has led FICORA to make changes to its regulations and recommendations by issuing new information security and reliability requirements for e-mail and Internet services.

In 2005, the aim is to expand cooperation between different actors still further and improve the processes for drawing up the analysis and disseminating information from it. Concrete steps include the updating and improvement of the CERT-FI and the FICORA websites so that analysis information can be disseminated more effectively. FICORA will include a section on malfunctions in the situation updates published by CERT-FI and use the feedback it receives for making the updates more useful for customers. FICORA will also improve its communications with CERT-FI, those responsible for operations in telecommunications companies, and those dealing with malfunctions, by purchasing different types of communications and information systems technology. The dissemination of dynamic information security analyses will be made more efficient by introducing RSS-feed channels for alerts and update information issued by CERT-FI, and SMS and alert services.

The manner in which information security threats are evolving and the fact that they can spread very rapidly means that information on them must also be available for users of mobile communications. Two separate systems are planned for mobile communications: for critical partners, an SMS/alert solution that will ensure the delivery of alerts to each partner, and for individual citizens and businesses, a service enabling customers to receive alerts as text messages on a cost-price basis. For real-time maintenance of links between authorities, encrypted video conferencing and VIRVE (Finland's Public Authority Network) telephones are to be introduced. There are also plans to purchase equipment and software for administering

The manner in which information security threats are evolving and the fact that they can spread very rapidly means that information on them must also be available for users of mobile communications.

group calls on VIRVE telephones and for establishing places of use. In order to facilitate the drawing up of the information security analysis and dissemination of its results, work on the TIKU information system will also be launched. The TIKU information system comprises systems connected with the processing and publication of analysis information. The overall impact and progress of the project will be tested during the TIETO 2005 exercise, the purpose of which is to produce analysis information for different customer segments that is as accurate as possible. However, it alone is not sufficient to eliminate information security risks faced by different actors. Each actor must assess its own information security risks and determine which functions are critical to the continuity of its operations.

Impact and modifications

The main impact of the project in 2004–2005 will be in the form of greater information security awareness and, consequently, an improvement in the national information security culture. If the results of the information security analysis can be disseminated to different customer segments in an efficient manner and in accordance with their needs, this will allow information security threats to be combated with appropriate and well-timed countermeasures in all customers segments, from telecommunications companies to private consumers. Problems arising from malfunctions can also be dealt with more efficiently and the risk of interruptions can be reduced. Threats to the critical infrastructure can also be identified and managed more easily. The project will also have a clear impact on information security cooperation, competitiveness, operating potential and risk-management because the analysis of national information security risks is highly useful in these sectors, too.

The project name clearly indicates that the aim is to produce segmented analysis information that is tailored to the needs of a large number of users and that enables threats to information security to be prevented or limited. Despite the introduction of a system for efficient preparation of information security risk analyses and dissemination of their results, it will remain the responsibility of each actor to identify the threat factors that are critical to the continuity of its operations. The purpose of the analysis is to assist in the identification of such threats, not to identify them on behalf of the actors. Careful consideration must continue to be given to the resources required for the analysis of national information security risks and dissemination of the results.



Project Chair

Ilkka Kananen

Deputy Director General
National Emergency Supply Agency
Pohjoinen Makasiinikatu 7 A
00130 Helsinki, Finland
Tel. +358 40 500 0238
firstname.lastname@nesa.fi

Secretariat

Hannu Sivonen

Project Secretary

National Emergency Supply Agency

Keith Bonnici

National Technology Agency of
Finland

Arsi Heinonen

Finnish Communications Regulatory
Authority (FICORA)

Terttu Mellin

Ministry of Finance

Juha Perttula

Ministry of Transport and
Communications

3.3. Methods for analysing vulnerability to information security risks

Aims and background

The objective of this project is to survey the current methods for analysing information security and to use this information as a basis for developing the methods further. To this end, the project will support and incorporate research aimed at making information infrastructure vulnerabilities more manageable. It will also help ensure that the knowledge and best practices generated by the research are available to the most important actors and organizations, thereby improving their risk management and facilitating their strategic planning in regard to secure information systems.

Ultimately, the development of methods for analysing information security vulnerabilities will make it easier to protect the critical infrastructure in the information society and to prepare for threats facing the country's most important information and communication systems.

The weaknesses and defects hidden in the different layers of information systems can cause delays for businesses and other operators using these systems, as well as resulting in errors and opening up opportunities for wilful damage and abuse. Such weaknesses and defects and the damage resulting from them are frequently reported, and sometimes they have serious consequences.

An analysis can only be successfully carried out if the vulnerability concerned has not yet been leaked to the public. Those carrying out the analysis must be able to rely on a cooperation network with international software suppliers, and independent analyses of the suppliers must also be available. Rapid reaction requires continuous alertness.

The parties to the process of analysing information security vulnerabilities can be grouped as follows:

- Those developing methods for identifying vulnerabilities (for example, the Oulu University Secure Programming Group)
- Those searching for vulnerabilities (software suppliers, research groups, independent researchers)
- National bodies analysing vulnerabilities and their impacts on a centralized basis and their international partners (CERT) and
- Those suffering from the effects of vulnerabilities (home users, organizations, critical infrastructure actors, authorities).

Home users, organizations, critical infrastructure actors and authorities must each assess the impact of vulnerabilities on their own operations. Organizations can outsource vulnerability analysis and the actions required to subcontractors.

The purpose of the project is to find and develop methods for identifying vulnerabilities and to find operational approaches and good practices supporting the above processes.

Situation in 2004 and progress in 2005

A public research project under the title Protos-Matine was carried out at the University of Oulu in 2004. It covered the management of information infrastructure vulnerability from the point of view of protocol dependency and was funded by the Scientific Board for National Defence and the National Emergency Supply Agency. The interim and final reports of the research project have been made available to the current project.

The purpose of Protos-Matine was to find methods for identifying vulnerabilities in telecommunications protocols. The focus was on situations where there are several products implementing the same protocol and on protocol families. Vulnerabilities often derive from common specifications or from common historic program code components. Background information for the project included protocol specifications and the source codes of the products using them, the history of different cases, the information possessed by experts involved in the specification work, and public interest on vulnerabilities. The historical information concerns the links between different specifications and implemented solutions, and the information provided by experts concerns which parts of the specifications involve compromises. Media-tracking analysis is one method of surveying the occurrence of vulnerabilities, while the Google search engine provided information about where different protocols are used.

In 2004, information was gathered on the research undertaken in information security analysis methods by universities. It was based on questionnaires carried out as part of the project and on publicly available sources:

- The Secure Programming Group at the University of Oulu's Faculty of Technology is researching ways of identifying vulnerabilities (one example of this is the Protos-Matine project) but is not analysing the impacts of vulnerabilities. The Department of Information Processing Science of the University of Oulu is studying methods for developing secure software and is also organizing courses on the topic.
- The Helsinki University of Technology is organizing basic courses on information security and a "hacker course" for those studying for a licentiate degree. It is also carrying out research on network technology security. In 2002, it conducted research on software verification, i.e. on comparing software against its specifications.
- No research on the subject was being carried out at the University of Helsinki, the Lappeenranta University of Technology, the University of Jyväskylä, the University of Tampere, the Tampere University of Technology or the University of Turku.

In 2005, the Protos-Matine project will focus on visualization methods and tools. Research funding for 2005 has already been granted by the Ministry of Transport and Communications and a funding application has been submitted to the Scientific Board for National Defence.

During 2005, the project programme will include examination of the most important telecommunications, system and information security actors in Finland (10–15), the vulnerability criteria they use, and methods and support available for the analysis processes described above.

Impact and modifications

Methods for analyzing information security are clearly needed. Attacks against information systems exploiting their vulnerability make the issue especially acute. In some cases these attacks mean concrete transfer of money to criminals or using computer capacity for criminal purposes.

Better methods for analyzing information security will make the identification of system vulnerabilities more effective and offer a way to rapid reaction, thus stopping damages from emerging or expanding. It is vital to increase awareness about information system vulnerabilities and to learn and use the analyzing methods.



Project Chair

Timo Lehtimäki

Head of Information Security
Finnish Communications
Regulatory Authority (FICORA)
PO Box 313, 00181 Helsinki
Finland
Tel. +358 50 514 8286
firstname.lastname@ficora.fi

Secretariat

Ilkka Kananen

Project Vice Chair
National Emergency Supply Agency

Lars Arnkil

VR-Group Ltd

Kimmo Bergius

Microsoft Finland Oy

Tapio Halkola

The Finnet Association

Erkki Heliö

TietoEnator Oyj

Ari Hyppönen

F-Secure Corporation

Pertti Hyvärinen

The Finnish Defence Forces

Esko Junnila

Digita Oy

Riku Kalinen

Finnish Security Police

Jani Kallio

Elisa Corporation

Jouni Keronen

Fortum Corporation

Juhani Lahti

Song Networks Oyj

Jorma Mellin

Ficix

Terttu Mellin

Ministry of Finance

3.4. Committee on Information Security in Critical Infrastructure

Aims and background

The objective of the Committee on Information Security in Critical Infrastructure is to put cooperation in the sector on a more efficient footing, to produce a survey of the actors in critical infrastructure, and to examine how best to improve information security and expand cooperation in the sector. The aim is to increase proactiveness while safeguarding the continuity of business operations in the event of malfunctions. A further aim is to promote cooperation between the actors in order to enhance their awareness of information security matters and to establish and disseminate best practices. Ensuring information security for the actors critical to the functioning of society at large can significantly enhance society's functioning in disruptive situations and thus improve public confidence in the functioning of society. Because there is a high degree of interdependency between electricity distribution and electronic communications, the Committee is also planning to produce a report on the impact of technology risks on communications services and electricity distribution and prepare proposals for appropriate measures. The Committee also aims to make the CERT operations of the Finnish Communications Regulatory Authority (FICORA) better suited for the needs of critical infrastructure.

Situation in 2004 and progress in 2005

Progress with the Committee's work is very slow, reflecting its long-term nature and the complexity and extent of the issues. Very few concrete results have been achieved so far. The Committee's objectives have been defined as surveying the available methods and establishing contacts with bodies that would be in a position to implement its proposals. The Committee may eventually develop into an instrument for more extensive cooperation and for implementing concrete forms of cooperation.

In surveying the existing actors and operations, it has become very clear that the issues dealt with are many and varied. Action and cooperation already exist in a variety of fields. As the problems are of a global nature, it has been deemed necessary to tackle them through international cooperation. Finland has been included in the CIIP list of NISCC (National Infrastructure Security Coordination Centre), the directory of which contains the contact information of bodies responsible for each country's critical infrastructure. International channels for exchanging information are thus being put on a stronger footing. The survey of actors and actions is being carried out at national level on the basis of the contacts established by the National Emergency Supply Agency, and the survey of the companies with priority classification has also started. The aim is to create an up-to-date list of contacts for the exchange of information on information security matters. The National Emergency Supply Agency has already produced a report on how these matters are dealt with in other countries. The report examines how different Western countries have defined and classified their critical infrastructure, what plans they have for protecting it and what factors have influenced the planning process. The aim is to clarify the concept of critical infrastructure, create an overview of the plans that have been prepared in different countries to ensure the functioning of critical infrastructure and to find out why the plans differ from each other. Because of its central role to the functioning of other infrastructures, some areas of the Critical Information Infrastructure (CIIP) are discussed separately.

The development of FICORA's CERT operations will also cover critical infrastructure. A technological adviser working in the CERT-FI group has been given specific responsibility for matters concerning critical infrastructure actors, and CERT-FI has also established an

Antti Paananen
Energy Market Authority

Rauli Parmes
Ministry of Transport and
Communications

Juhani Porthan
Ministry of the Interior

Timo Ristikankare
Fingrid

Nils Rostedt
Oy LM Ericsson Ab

Antti Tassberg
Nokia Group

Mikko Viitasaari
TeliaSonera Finland Oyj

Timo Ylitalo
The Finnish Bankers' Association

e-mailing list for actors represented on the Committee. The list, which is on a trial basis, may be extended to cover the whole CIP field in the future. The list enables concrete information to be disseminated on such matters as vulnerabilities in the sector and advance information on vulnerabilities. The manner in which information security threats are evolving and the fact that they can spread very rapidly means that information on them must also be available for users of mobile communications within the critical infrastructure. Two separate systems are planned for mobile communications: for critical partners, an SMS/alert solution that will ensure the delivery of alerts to each partner, and for individual citizens and businesses, a service enabling customers to receive alerts as text messages on a cost-price basis. For realtime maintenance of links between authorities, encrypted video conferencing and VIRVE telephones are to be introduced. There are also plans to purchase equipment and software for administering group calls on VIRVE telephones and for establishing places of use.

The FICORA CERT-FI group is also participating in events such as the Risk Management Fair to heighten awareness of the importance of information security risk management. FICORA has also started work to expand cooperation and disseminate information. The aim is to set up a CIP section on the FICORA website, which would present a selection of the best practices, checklists and information security guidelines. The threats facing critical infrastructure are similar to those facing other information systems, varying somewhat according to the software and services they use. The threats are often connected with software vulnerabilities that enable intruders to target a system for undesirable action (such as information security breaches and DoS (denial of service) attacks. With a DoS attack, an intruder may try to cripple essential information systems, either by targeting the system directly or by targeting the information network or part of it that is connected with the critical infrastructure system. When securing critical infrastructure information systems, account must be taken of direct and indirect threats and the action that can be taken to combat both types of threat.

The action already launched will be accelerated during 2005 and, partly as a result of increasing awareness, concrete results can also be expected. A report on the impact of technology risks on communications services and on electricity distribution and proposals for managing the risks will probably require work to be commissioned from a consultant, which will include the formulation of proposals. Even though the Committee would act as the steering group, the work itself should, as far as possible, be carried out by consultants. During 2005, the Committee aims to become a channel for cooperation and a forum for disseminating best practices to critical infrastructure actors. In 2005, the focus will be on improvements in the information security of SCADA (Supervisory Control and Data Acquisition) systems. The Committee has also begun to monitor the progress of the project *Honeypots for SCADA and industrial networks*.

Impact and modifications

The Committee started its work in 2004 and the increased information security awareness and effective dissemination of best practices are expected to produce concrete results during 2005. The project needs a larger number of active participants and requires a great many studies to be carried out so that all aspects of this wideranging field can be covered. The project should also be allocated funding for some of the research work to be carried out by consultants.

4. Safeguarding fundamental rights and protecting the nation's knowledge capital

The construction of a secure information society cannot be at the expense of the fundamental rights and liberties of individual citizens and other actors. In a secure information society, all actors must have assurances that their information and messages are relayed, processed and stored confidentially and will not end up in the wrong hands. Furthermore, everyone must have easy access to the information they are authorized to use.

In companies, security priority is given to business secrets, customer information and product development information. To this end the following measures will be implemented.





Project Chair

Sanna Helopuro

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28608
Mobile +358 400 515 548
firstname.lastname@mintc.fi

Secretariat

Eeva Lantto

Finnish Communications
Regulatory Authority (FICORA)

Tapani Tarvainen

EFFI ry

Leena Vettenranta

(presented an opinion)
Ministry of Justice

Sari Kajantie

(presented an opinion)
National Bureau of Investigation

4.1. Ensuring fundamental rights

Aims and background

Fundamental rights are the individual rights laid down in the Finnish Constitution. Only basic rights of special importance are considered fundamental rights. They are characterized by a special permanence and legal standing, as they represent the basic values of our justice system. Thus, the building of a society with a high level of information security cannot be at the expense of fundamental rights of individuals and other actors. A large number of provisions that can be characterized as information security legislation have been incorporated in the Finnish statute books in recent years. There are many acts and decrees that have information security relevance, even though they do not contain explicit references to the matter. These include legislation on privacy protection. The Finnish Constitution, too, contains a number of provisions on fundamental rights that are also relevant from the information security point of view.

As more and more emphasis is put on fundamental rights, the legal aspects of different phenomena are being examined from new perspectives. One may even talk of judicial interpretation being obligated to take account of fundamental rights rather than being favourably disposed towards fundamental rights. How faithfully are different fundamental rights then observed in the new information infrastructure and is there any need to create new fundamental rights for the new digital operating environment? Research on the legal aspects of information security is a relatively new phenomenon, and even though information security has been given consideration in the legislation on the personal data protection from an early stage, there has been little interest in the topic within jurisprudence.

The aim of this project is to assess how well fundamental rights provisions are observed in the information security legislation, guidelines and standards issued by the authorities, and electronic services provided by different authorities. Special attention will be given to how well such fundamental rights as freedom of speech, confidentiality of communications and right to privacy are observed. Thus, the project will verify that the information security legislation, guidelines and standards issued by the authorities, and electronic services provided by different authorities has been in accordance with fundamental rights provisions and ensure that they are in the future. Any inadequacies or ambiguities should be highlighted during the assessment.

Situation in 2004 and progress in 2005

The working group held its first meeting in June 2004, which also marked the start of the project.

The working group has launched two studies to examine how much consideration is given to freedom of speech, right to privacy and other fundamental rights in the legal provisions on information society services, electronic communications and security, and in guidelines issued by the authorities and electronic services provided by the authorities. This is the first time the consideration of fundamental rights in information security has been studied, which makes the survey work an extremely challenging undertaking. After all, there are few experts in Finland specializing in this area. In the first study, the focus will be on the analysis of the practical impact of information security legislation on fundamental rights, while the second study will take a more theoretical approach. The Ministry of Transport and Communications has budgeted EUR 42,000 for the studies.

The purpose of the surveys is to examine how much consideration is given to freedom of speech, right to privacy and other fundamental rights in the legal provisions on the information society services, electronic communications and security, and in guidelines issued by the authorities and electronic services provided by the authorities.

Impact and modifications

The aim of the project is to examine how well the legislative framework on information security, guidelines issued by the authorities and electronic services observe the fundamental rights provisions. The project covers some of the same issues as the project dealing with assessing the impact of the legislation, because in principle both are dealing with provisions based on fundamental rights. However, the tight schedule for the studies does not allow a comprehensive review to be prepared and therefore, these studies should be followed by more extensive studies involving an in-depth analysis of the relationship between fundamental rights and different regulatory categories.

Originally, the project was also intended to cover the relationship between fundamental rights and the huge number of existing information security standards. However, even though these standards would undoubtedly be an interesting area for study, the working group decided not to include them in its studies at this stage. The standards should perhaps be made part of the project on certificates, as the two issues are closely related.



Project Chair

Sanna Helopuro

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28608
Mobile +358 400 515 548
firstname.lastname@mintc.fi

Secretariat

Erkki Heliö

TietoEnator Oyj

Urho Ilmonen

Nokia Group

Sari Kajantie

National Bureau of Investigation

Markku Mäenpää

National Archives

Kari Summanen

National Board of Patents and
Registration

Ilkka Vuorenmaa

Anti-Piracy Centre in Finland

4.2. Protection of national knowledge capital

Aims and background

The fact that the markets for knowledge production and use are on a global scale means that knowledge and the ability to process it are becoming increasingly valuable assets. In a technologically advanced and networked world, the rapid flow of information across national borders makes it easier for organizations to function but also generates pressure to make information more secure. It must be possible to prevent important knowledge capital from leaking to outsiders. At the same time, one should remember that not all knowledge capital of great national value requires protection for the reason that it may be leaked or may disappear but because the preservation and permanence of the material must be guaranteed. The concept of “knowledge capital” covers a very wide spectrum. Listing the nation’s important knowledge capital assets is also a huge challenge, as different organizations do not always agree on what the term actually covers. It is becoming increasingly difficult to identify those key factors that enable the national knowledge capital to be protected in a manner that satisfies all organizations involved.

The objective of this project is to produce an overall assessment of the protection of national knowledge capital and consider the situation and modifications of both the private and public sectors. The aim is to produce a realistic picture of what kind of knowledge capital is deemed nationally important, whether or not enough attention has been paid to the protection of knowledge capital and what could be done to protect it in the future. A further aim is to survey the most serious information security risks threatening Finnish knowledge capital in the future, and examine how the situation could be improved and how the information security risks could be reduced.

The project must help to ensure that national knowledge capital is protected against any outside intrusion and is securely accessible to all authorized users. With the measures drafted as part of the project, the aim is to ensure the long-term protection of the national knowledge capital. In addition to having the specific targets referred to above, the project also aims to make organizations more aware of information security and encourage them to make their operations more secure.

Situation in 2004 and progress in 2005

As already noted, knowledge capital is a broad concept but of great importance for the progress of the project. Knowledge capital can be divided into human capital (staff competence, motivation and commitment), immaterial capital (data, information, intellectual property, and the organization itself) and the strategic reserve (the ability to produce and commercialize innovations). As the working group was of the opinion that such matters as staff competence, motivation and commitment do not need the protection envisaged in the project, it was decided to limit the scope of the concept.

The working group took the view that for the purposes of the National Information Security Strategy, knowledge capital means immaterial capital as defined above. This type of knowledge capital comprises systematically created conceptual information that is essential to the operations and basic tasks of an organization, such as innovations, inventions, technical specifications and drawings, methodologies, software, applications, documents and other information items. In addition to these, information such as business secrets, customer information and product development information also belong to the knowledge capital essential to the operations of a company. In the government sector, immaterial capital can include base registers maintained by the authorities that contain information about matters important to the

The survey of Finland's national knowledge capital will help to define the elements of knowledge capital that should be considered of national importance and should be protected through collective efforts and made more secure.

functioning of society at large. Knowledge capital falling within the sphere of privacy protection for individual citizens is also an important part of the concept of knowledge capital.

In autumn 2004, the working group began a study aimed at providing it with clear answers to such questions as what type of knowledge capital is considered of national importance, has enough been done to protect it and what could be done to protect it in the future. The group will also examine the information security risks that pose a major threat to Finland's knowledge capital in the future as well as the ways of improving the situation and of reducing the risks. The Ministry of Transport and Communications has budgeted EUR 18,000 for the survey.

Impact and modifications

The survey of Finland's national knowledge capital will help to define the elements of knowledge capital that should be considered of national importance and should be protected through collective efforts and made more secure. It will also make different organizations more aware of the importance of knowledge capital and of the need to protect it. The proposed measures put forward as part of the project should also list the action that would enable individual companies and the government sector to protect knowledge capital more effectively.

The project has already attracted interest in the media. The media interest has been fuelled by cases involving the disclosure of business secrets.

Project Chair

Sari Kajantie

Chief Superintendent
National Bureau of Investigation
PO Box 285, 01301 Vantaa
Finland
Tel. +358 9 8388 6267
firstname.lastname@krp.poliisi.fi

4.3. Cybercrime as an information security problem

Aims and background

Cybercrime involves high potential benefits, carries a relatively small risk of being caught and often requires only limited resources. As societies are becoming increasingly network-based, both the damage caused by cybercrime and the benefits that can be obtained through such action are on the increase. Small risks and inputs and huge potential rewards make cybercrime highly attractive, especially if the aim is to reap financial benefits. Crime therefore poses a real threat to the functioning of a networked society unless efficient measures are taken to combat it.

The best way to combat cybercrime more effectively is by improving protection and by increasing the likelihood of capture. The aim of this project is therefore to tackle cybercrime by putting crime investigation and crime prevention on a better footing. Improved preventive protection can also increase the likelihood of being caught. Such preventive protection includes improving the security of unprotected home computers.

The detection rate for cybercrime will improve if more attention is paid to combating such crime by carefully targeting investigation resources and developing legal and forensic tools that keep pace with changes in the criminal environment.

Successful crime prevention requires appropriate measures, a large amount of accurate information, and alertness among those maintaining information systems. The public debate about information security has mainly focused on how to protect against malicious software that chooses its targets randomly. Even though such software is harmful, it is nevertheless only a consequence of the real problem, which is the use of vulnerable software and systems that lack security in their design. If the real problem is ignored, it can be difficult to protect against targeted attacks.

Thus, the measures proposed for this project come in two sections:

- Section A contains measures for making cybercrime investigation more effective
- Section B focuses on the prevention of cybercrime

The measures only cover cybercrime that is deemed an information security problem and that also targets information systems. Other criminal acts carried out using networked services, such as messages relayed through the network as part of organized drug trade or using a personal computer for distributing illegal material, are not considered here. This is because in these areas the violation of the object of legal protection does not primarily concern “Pax Computationis” and neither can improved information security provide any protection against such acts.

Section A: Making cybercrime investigation more effective

The following two measures aimed at making cybercrime investigation more effective will be selected for closer examination:

- a) The IT Crime Unit of the National Bureau of Investigation will, on the basis of the Internal Security Programme of the Ministry of the Interior and the lessons learned by investigators specializing in computer crime, draw up a proposal for a nationwide strategy for combating computer crime. The proposal would contain concrete measures enabling the police to make more effective use of tactical and forensic investigation, criminal intelligence and other preventive measures when combating new types of crime. If the proposal is approved, the measures contained in it will be put into effect, as available resources permit.
- b) In order to ensure overall effectiveness of cybercrime investigation, the Ministry of the Interior, the Ministry of Transport and Communications and the Ministry of Justice will take part in the drafting of the framework decision on data retention, to be carried out by the Council of the European Union's working party on cooperation in criminal matters.

The preparation of section A will not involve bodies outside the government sector or require additional funding. Under section 24(1)(5) of the Act on the Openness of Government Activities (621/1999), the documentation involved in developing cybercrime investigation is confidential. The framework decision necessitating legislative changes and the proposals for framework decisions drawn up during the preparatory stage are, however, public documents.

Section B: Preventive measures

The prime purpose of the reports to be drawn as part of section B is to publicize the information security threat posed by cybercrime in a way that helps business and public administration actors and private consumers to secure their networked systems and the information contained in them. Section B consists of two measures.

a) Phenomena report

The IT Crime Unit of the National Bureau of Investigation (Project Chair Kajantie) will prepare a report on the criminal phenomena affecting networks, the way they usually occur, the motives behind them, potential victims, impacts of the crimes and how best to protect against them.

b) Topical report

Using the phenomena report as a basis, a group of experts will prepare a topical report describing what types of vulnerability are being exploited at the moment and presenting some of the criminal purposes for which the vulnerabilities are used. The report will also describe any measures to be taken to combat the threats and reduce their impacts.

The members of the working group will include representatives from Government security organizations, the Ministry of Transport and Communications and top network technology experts from the universities, the Finnish information security industry and elsewhere in the private sector.

The purpose of the measures drawn up as part of the crime investigation section is to prepare for a situation in which serious and organized crime is becoming increasingly network-based, to ensure that cybercrime can be investigated anywhere in the country and to ensure that it can also be investigated in the future.

Both section B reports will be made public so that they can be of maximum use in the protection of systems and knowledge capital. The material processed by the working group during the preparatory stage may, however, be kept confidential in whole or in part, as laid down in section 24(1) of the Act on the Openness of Government Activities (621/1999) or as agreed with the bodies submitting the material.

The preparation of the phenomena report will not involve bodies outside the government sector or require additional funding. Likewise, the drawing up of the topical report will only involve the parties invited to the working group.

Impact and modifications

Section A:

- The work on the proposal for a cybercrime investigation strategy to be submitted to the Ministry of the Interior was completed on 9 July 2004 and the document was presented to the Supreme Police Command on 24 September 2004.
- The EU working party on cooperation in criminal matters started drafting the Council framework decision in summer 2004 and the work should be completed by July 2005.

Section B:

- The phenomena report was still under preparation in autumn 2004.
- The working group drawing up the topical report will be convened as soon as the work on the preliminary report is complete.

An assessment of the impact of the measures in 2004–2005

The purpose of the measures drawn up as part of the crime investigation section is to prepare for a situation in which serious and organized crime is becoming increasingly network-based, to ensure that cybercrime can be investigated anywhere in the country and to ensure that it can also be investigated in the future.

In section B, which focuses on preventive measures, the aim is to encourage those maintaining information networks to protect their own and their customers' information systems against known malicious software and targeted attacks.

Success in combating cybercrime will be measured using the police administration's own internal indicators. No quantitative indicators are proposed for evaluating crime prevention because cybercrime mostly goes unreported: not even the injured parties may be able to identify computer network criminals unless they have particularly skilled system maintenance staff. On the other hand, injured parties who detect a crime may be unwilling to become involved in a criminal process, which means that the case is not entered in the statistics. Thus, for example, the figure showing the variation in the level of reported cybercrime is not a good indicator of the effectiveness of crime prevention.

The section on making cybercrime investigation more effective is independent in relation to other projects. The section on crime prevention is partly about the same issues as in project 4.1. (*Ensuring fundamental rights*) and is closely linked to the problems discussed in project 4.2. (*Protection of national knowledge capital*). Of the other projects, project 3.3 (*Methods for analysing vulnerability to information security risks*) is highly relevant to the prevention of cybercrime. In principle, project 3.1. (*Assessing and more effectively combating information security risks*) is also relevant to the cybercrime project but, as it takes an entirely different approach to the topic, it may produce results that are not entirely consistent with this project.

5. Increasing information security awareness and competence

Information security competence has become a new civic skill. In a secure information society, all actors must be aware of the information security risks of their actions and of their own role in preventing them.

The National Information Security Strategy is intended to raise the level of information security competence by investing in the expertise of information security professionals and in the general information security awareness of all actors. To this end, the following measures will be implemented.





Project Chair

Markku Suvanen

Senior Adviser
Ministry of Education
PO Box 29, 00023 Government
Finland
Tel. +358 9 160 77397
Mobile +358 40 525 0091
firstname.lastname@minedu.fi

Secretariat

Ritva Kivi

National Board of Education

Merja Malkki

Finnish Federation for
Communications and
Teleinformatics (FICom ry)

Terttu Mellin

Ministry of Finance

Juha Nummela

Statistics Finland

Tapio Virkkunen

Ministry of Transport and
Communications

5.1. Charting and developing information security awareness and competence

Aims and background

The purpose of this project is to chart, as extensively as possible, the level of information security awareness and competence among individual citizens and organizations, particularly educational institutions, and to define the target level of competence and launch projects for improving general information security competence and improving the training for information security professionals. This work will be carried out by gathering existing information and by including questions on information security in questionnaires for individual citizens and organizations. The collection of information from individual citizens will be in the form of appendices to Statistics Finland questionnaires. Questions on information security directed at educational institutions will be included in the information society section of the education survey conducted by Statistics Finland every autumn. For other organizations, surveys and studies will be carried as necessary. The aims of improving general information security competence, providing better training for information security professionals and improving information security in the operational environment of educational institutions are all part of the implementation of the Information Society Programme for Education, Training and Research 2004–2006 drawn up by the Ministry of Education.

By gathering information as outlined above, it will be possible to assess the level of general information security awareness and competence among individual citizens and organizations and to judge the situation more accurately. It will also be possible to form a common view of the information security skills that are needed at different levels and in different situations. Information security matters will be made part of general information and communications technology teaching at different levels, and every effort will be made to ensure that the training of information security professionals is in accordance with the need. A project cooperation group has been set up to implement the proposed measures, and in principle the term of the group will extend over the whole implementation of the National Information Security Strategy. Surveys and studies have already been started by different bodies as part of the process of implementing the project, and the survey results will be reported to the Advisory Board on an annual basis.

Situation in 2004 and progress in 2005

The project cooperation group began its work in spring 2004 and held a number of meetings during the year with the cooperation group of project 5.2. (*Improving people's information security awareness*). Reports prepared by bodies involved in the projects have been presented at the meetings, and plans for further action discussed, particularly the content of future surveys.

To obtain an overview of information security awareness and competence among individual citizens, Statistics Finland included questions about information security in an interview survey in spring 2004. The results can be found in the Statistics Finland report on Finnish People's Communication Capabilities in Interactive Society of the 2000s (Bulletin of Statistics 2004/4). They show that the measures recommended in spring 2004 had been incorporated in most home computers. For example, 90 per cent of all home PCs with a Windows operating system were reported to have or probably have the latest information security protection, while in about 70 per cent of all home PCs incoming e-mail is checked for viruses, and more than 80 per cent of all home PCs with a broadband connection are equipped with a firewall. The survey should be repeated in 2005 so that the situation can be constantly monitored. At the same time, the questions on technical information security should be accompanied by questions designed to

give a fuller picture of information security awareness and competence. Such questions are planned for inclusion in the 2005 surveys.

Questions on information security in educational institutions were included in the information society section of the education survey conducted by Statistics Finland in the autumn of 2004. The results will be made available during 2005 and recommendations for educational institutions based on them could be issued the same year. The Ministry of Education is to carry out a separate information society survey for institutes of higher education (universities and polytechnics). This survey will be carried out in early 2005 and will also include questions on information security.

Implementation of the *Information Society Programme for Education, Training and Research 2004–2006*, drawn up by the Ministry of Education, has begun with the appointment of an advisory board and a secretariat. The programme includes measures on information security: promotion of information security in educational institutions, development of information security training and the improvement of information security awareness and competence among individual citizens. The National Broadband Strategy also contains measures targeting educational institutions, such as improvements in network connections at schools. The impacts of these national strategies and programmes should be closely monitored, and more questionnaires should be carried out in educational institutions during the next few years.

Impact and modifications

Surveying and developing information security awareness and competence can be divided into two areas, one dealing with organizations and the other with individual citizens. For organizations, the action plan includes projects specifically targeting companies (2.2.) and the public administration (5.3.). In this project, the focus should be on examining, developing and monitoring the state of information security in educational institutions. The provision of information to educational institutions can be made in connection with the National Information Security Day project (5.5.). Assessment of information security awareness among individual citizens is closely connected to the efforts to improve people's information security awareness, for which there is already a project (5.2.), although it has been suggested that this should be removed as it duplicates work carried out in the National Information Security Day project.



Project Chair

Markku Suvanen

Senior Adviser
Ministry of Education
PO Box 29, 00023 Government
Finland
Tel. +358 9 160 77397
Mobile +358 40 525 0091
firstname.lastname@minedu.fi

Secretariat

Pirjo Immonen-Oikkonen

National Board of Education

Terttu Mellin

Ministry of Finance

Oili Salminen

Finnish Information Society
Development Centre (TIEKE)

Mari Suhonen

The Finnish Terminology Centre
(TSK)

Tapio Virkkunen

Ministry of Transport and
Communications

5.2. Improving people's information security awareness

Aims and background

The purpose of this project is to make individual citizens more aware of information security matters by providing them with relevant information, preparing media campaigns and by incorporating information security matters in curricula at all levels of education. All educational institutions will also be provided with information about the best practices to enable them to improve their awareness of the subject. A comprehensive vocabulary containing all basic information security concepts will also be drawn up. It will contain definitions for the most commonly used concepts and provide recommendations on the usage of the Finnish terms. People's information security awareness will also be improved through the distribution of material and the publicity campaign in connection with the National Information Security Day. Information security training at educational institutions and the process of improving their awareness of the issues are included in the Information Society Programme for Education, Training and Research 2004–2006 drawn up by the Ministry of Education. The education administration plans to incorporate information security matters into the basic curricula of general education and vocational training, as part of the overall teaching on information and communications technology. All educational institutions will also receive information about the safe use of the Internet.

The project will help improve individual citizens' awareness of and competence in information security matters. At the same time they will learn how to make practical use of their information security skills. Annual interview surveys carried out by Statistics Finland will be one way of monitoring the situation.

A cooperation group dealing with the improvement of information security awareness among individual citizens has been set up to implement the measures proposed as part of this project, and in principle the term of the group will extend over the whole implementation period of the National Information Security Strategy. However, any reorganization of the projects carried out as part of the Strategy will have a decisive impact on the future and length of term of the working group. Different bodies have already started implementing the project and the results will be reported to the Advisory Board on an annual basis.

Situation in 2004 and progress in 2005

The project cooperation group began its work in spring 2004 and held a number of meetings during the year with the cooperation group of project 5.1. (*Charting and developing information security awareness and competence*). Situation reports prepared by bodies involved in the project have been presented at the meetings and plans for further action discussed, particularly the content of future surveys.

In order to increase information security awareness and competence among individual citizens, the project has been made part of the National Information Security Day project, which distributes facts and material about information security to the general public. The 2004 campaign succeeded in heightening public awareness about the problem, and it is hoped to repeat this in 2005.

A working group coordinated by the Finnish Terminology Centre (TSK) has completed work on an information security vocabulary, named Tiivis tietoturvasanasto (Compact Vocabulary of Information Security). The working group comprised experts from Elisa Corporation, the Finnet Association, F-Secure Corporation, the Ministry of Transport and Communications, TeliaSonera Finland Oyj and the Finnish Communications Regulatory Authority. The vocabulary was published in autumn 2004 by Taloustieto Oy.

The National Board of Education has continued to disseminate information about information security through various channels, such as the EDU.fi service intended for teachers and the OTE magazine. It will also take part in the *National Information Security Day 2005*, which will focus on comprehensive schools.

Impact and modifications

There are still overlaps in the awareness projects of the action plan. These should be removed, and the target groups redefined. For example, the measures directed at private individuals could be made a separate entity.

The cooperation group therefore proposes that this project (5.2.) be terminated as a separate undertaking, as its objectives have already been achieved (for example, the information security vocabulary) or will be dealt with in connection with other projects, especially project 5.5.



Project Chair

Terttu Mellin

Senior Officer
Ministry of Finance
PO Box 28, 00023 Government
Finland
Tel. +358 9 160 33214
Mobile +358 40 820 3254

5.3. Information security awareness in public administration

Aims and background

The aim is to improve information security awareness in the government sector and the municipal sector.

More instructions and guidelines will be issued. The project is being run in connection with other projects aimed at increasing awareness of information security. The Public Management Department at the Ministry of Finance is responsible for general guidance and development on government information security. The Department's principal activities in information security guidance include issuing government guidelines on information security, arranging joint projects on information security, cooperating at national and international levels, and the diverse activities of the Steering Committee for Data Security in State Administration (VAHTI) set up by the Ministry of Finance covering all areas of information security and all branches of government.

Situation in 2004 and progress in 2005

As in section 2.4.

Impact and modifications

As in section 2.4. It has been found necessary to combine projects 2.4. (*Standardizing public-sector information security procedures*) and 5.3. (*Information security awareness in public administration*). Harmonization and awareness are and should be promoted jointly and not separately.



Project Chair

Juha Perttula

Ministerial Adviser
Ministry of Transport and
Communications
PO Box 31, 00023 Government
Finland
Tel. +358 9 160 28617
Mobile +358 400 694 419
firstname.lastname@mintc.fi

Secretariat

Leena Haapaniemi

SFS-Inspecta Certification

Tarja Helkamäki

Elisa Corporation

Sami Kilkkilä

Finnish Communications
Regulatory Authority (FICORA)

Riitta Kokko-Herrala

Consumer Agency

Sami O. Koskinen

Helsinki University of Technology

Arja Terho

Ministry of Finance

Leena Tikkanen

Centre for Metrology and
Accreditation

5.4. Certificates

Aims and background

A large number of different information security certificates are available. However, actors know too little about them and make too little use of them, which means that they are unable to take full advantage of the potential benefits. Another problem is that no comprehensive surveys have been made on the topic.

The aim of the project is that the different actors, such as equipment manufacturers, users and consumers, should be as fully aware as possible of the information security certificates that would be of use to them. The aim is to ensure that different actors are able to take better advantage of the certificates. The project will promote the development and use of information security certificates and make users and consumers more aware of the role the certificates play in the construction of different systems and in the purchasing of different products and services. The intention is to produce a comprehensive report about national and international information security certificates applying to users, products and systems. Another aim is to identify problems related to awareness and use of certificates and to assess the measures for promoting such awareness and use.

Situation in 2004 and progress in 2005

The project implementation plan was presented to the *National Information Security Advisory Board* on June 15, 2004, and the project working group started its work in May 2004. In 2004, a comprehensive survey of existing certificates was carried out. The working group will assess the need to promote the use of certificates and to make users and consumers more aware of them, and it also aims to present proposals for any measures that might be necessary.

A study commissioned from consultants in support of the group's work was completed at the end of October 2004. The study included a survey of all existing information security certificates and detailed consideration of the uses of such certificates, taking into account such matters as the development of on-line shopping, the extent of use of certificates, the consumer perspective, the viewpoint of staff in different companies and organizations, marketing and purchasing.

The consultants' study identified a total of nine different product and service certificates (plus a number of products resembling certificates), two system certificates and 86 personal certificates. Of the personal certificates, 53 were product-independent, and 33 product-specific. The information security certificates can be divided into different categories. Service certificates are certificates that can be granted to services meeting the information security requirements set and verified by the body granting the certificate. Product certificates are, correspondingly, certificates that can be granted to products meeting the information security requirements set and verified by the body granting the certificate.

System certificates are certificates that can be granted to systems (for example, information security management systems) meeting the requirements set and verified by the body granting the certificate, and personal certificates are certificates that can be granted to individuals meeting the information security requirements set and measured by the body granting the certificate. Personal certificates can further be divided into product-independent and product-specific certificates.

Based on the study, the working group will draw up recommendations concerning the promotion of certificate use and proposals for any other measures needed. The opinions expressed by the consultants in their study will not necessarily be consistent with the final views of the working group. For example, the consultants were of the opinion that service certificates could bring genuine benefits, for instance to consumers. However, they added that the

unpopularity of such certificates is not the main reason for the slow increase in on-line shopping. There are many different labels resembling service certificates on the market, which promise consumers and other groups independent arbitration in disputes. However, in regard to Common Criteria, it is more important to ensure smooth cooperation with foreign testing laboratories than to insist on the use of a Finnish testing institute.

The large number of personal certificates is undoubtedly one factor hampering the spread of such certificates. It is not always possible to identify the most important certificates and there is a reluctance to invest in less-known certificates. Moreover, there is still relatively little awareness of different information security certificates. Information security on home PCs involves so many factors that it cannot be dealt with by product certificates alone. For those working at the customer interface, it is important to be able to demonstrate the advantages of their own company over the rivals. Verbal assurances are not always enough, however; certificates granted by third parties are needed, too.

Certificates for different information security products are also granted by purely commercial actors whose certificates are not based on generally accepted criteria. Developing product, service or system certificates is a challenging task, and gaining widespread acceptance requires hard work and is far from certain. CC, FIPS and ITSEC product certificates only apply to certified versions of software or hardware; strictly speaking, they only cover certain configurations. However, in the case of Common Criteria, certification of Flaw Remediation Assurance is also possible.

In business, factors such as the reputation of the company, its references and its financial situation are more important than information security certificates. This probably also applies to consumers doing on-line shopping. System certificates are probably most useful in situations in which the customer is another company or organization. For most personal certificates, it is almost essential for the applicant to take part in courses on the use of the certificate, as participation in such training can bring a substantial reduction in the purchase price of the certificate.

All current information systems are networked to a greater or lesser degree. A large number of Protection Profile documents are available that are compatible with Common Criteria and can be combined into large product-independent system entities. However, despite the existence of different standards and certificates, and even though security-certified products are used as building blocks for networked information systems, there are no precise methods for assessing the information security of such systems.

On the basis of the consultants' study and the views presented in it, the working group will examine the matter further and, if necessary, draw up proposals for improvements in information security certificates. The consultants' study was funded by the Ministry of Transport and Communications. In 2004, a total of EUR 19,200 in R&D funds was spent on the project.

Impact and modifications

This project is partly about the same issues as project 5.5. (*National Information Security Day*). Information security certificates can be used in a multitude of ways to ensure and assess the level of information security. The purpose of the project is to ensure that different actors make better use of the certificates. If this becomes reality, companies, public administration, equipment manufacturers, system maintenance bodies and end users could all benefit from improvements in information security.

Assessments will be carried out on how the project results can form a basis for cooperation between the project working group and other National Information Security Strategy projects on improving information security awareness and on international cooperation. The impact of the project will largely depend on how effectively its proposed measures and views can be disseminated to different actors.



**Project Chair
Nora Elers**

(up to 8 November 2004)
Communications Manager
Finnish Federation for
Communications and Teleinformatics
(FiCom ry)
Korkeavuorenkatu 30 A
00130 Helsinki, Finland
Tel. +358 9 6812 1015
firstname.lastname@ficom.fi

Project Chair

Anna Lauttamus-Kauppila
(from 8 November 2004)
Finnish Communications
Regulatory Authority (FICORA)
PO Box 313
00181 Helsinki, Finland
Tel. +358 9 6966 404
firstname.lastname@ficora.fi

Project Chair

Kristiina Klemetti
(from 8 November 2004)
Communications Manager
Finnish Federation for
Communications and
Teleinformatics (FiCom ry)
Korkeavuorenkatu 30 A
00130 Helsinki, Finland
Tel. +358 9 6812 1015
firstname.lastname@ficom.fi

5.5. National Information Security Day 2005

Aims and background

Finland's National Information Security Day is an annual event held in February. It is organized jointly by various public-sector bodies, private-sector businesses and other organizations. The purpose is to increase awareness of current threats to information security and the practical ways of protecting against these threats.

The first National Information Security Day was held on 11 February 2004, and the aim was that everyone with a home PC linked to the Internet would ensure that their operating system had the latest information security updates, current anti-virus software and a firewall.

The 2004 event was a success: according to surveys by Taloustutkimus Oy and Statistics Finland, both anti-virus software and firewalls were installed in a significantly greater number of home PCs in April 2004 than in the previous autumn.

The next National Information Security Day will be on February 8, 2005 and is targeted especially at schoolchildren and their teachers and parents. On the day of the event, material on information security and secure use of the Internet will be prominently featured in comprehensive schools, and children will also have information to take home with them. The patron for the event will be the Minister of Education, Tuula Haatainen. Alongside the material for schools, there will also be an extensive national publicity and marketing campaign, ensuring that the event is truly a National Information Security Day.

Situation in 2004 and progress in 2005

To help prepare for the National Information Security Day, a web service designed to support information security teaching in comprehensive schools was launched on 15 November 2004, and was widely publicized among teachers. The address of the web service, available in both Finnish and Swedish, is www.tietoturvakoulu.fi. Various teaching, ICT, information security, law and child welfare professionals were involved in setting up the web service.

The web service is divided into separate sections for teachers, younger and older children, and parents. The teachers' section includes readily comprehensible teaching material on information security. The material is presented in illustrated and convenient form and it can also be printed out if necessary. Links are available, too, allowing teachers to find more details on information security technologies, for example at www.tietoturvaopas.fi (in Finnish and Swedish). The service also includes an option for requesting an information security expert to come and talk to teachers and parents free of charge about the basics of secure Internet use, for instance at teacher meetings, parents' evenings and meetings of parents associations. These information security experts are representatives of the various participants in the project.

The sections of the web service designed for comprehensive school pupils make good use of the diversity of the Internet. Stories targeted at different age groups have been designed as cartoon-like animations and incorporate information security advice, points to mull over, and lots of different tasks. These pages are designed to be accessible from most browsers and computers. On National Information Security Day (8 February 2005), an information security competition will be launched. The competition will be open to all comprehensive school pupils in Finland (i.e. up to the ninth grade) and the winners will be announced at the end of the school year.

Management Group:

Nora Elers

(up to 8 November 2004)

Project Chair

Finnish Federation for Communications and Teleinformatics (FiCom ry)

Anna Lauttamus-Kaupila

(from 8 November 2004)

Project Chair

Finnish Communications Regulatory Authority (FICORA)

Pirjo Immonen-Oikkonen

National Board of Education

Kristiina Klemetti

(from 8 November 2004)

Finnish Federation for Communications and Teleinformatics (FiCom ry)

Suvi Kuikka

Save the Children Finland

Anita Ovaska

Elisa Corporation

Timo Saxén

TeliaSonera Finland Oyj

Jaana Sirkiä

F-Secure Corporation

Tiina Vuorio

Microsoft Oy

Project Coordinator:

Sari Salmela

Finnish Communications Regulatory Authority (FICORA), part-time

Other participants in project working groups:

Johanna Anttila

Ministry of Transport and Communications

Juha Aromaa

The Mannerheim League for Child Welfare

Jussi Autio

The Finnet Association

Kimmo Bergius

Microsoft Oy

Katrina Harjuhahto-Madetoja

Information Society Programme

Information Security Day for everyone

To ensure the continued and efficient development of Finland's information society, it is very important that people have a better understanding of the Internet's benefits and potential harm. Practical computer competence should be part of everyone's basic skills. This is why National Information Security Day 2005 will be publicized widely both in schools and outside the school environment. During the weeks preceding the event there will be TV advertising campaigns on the subject of information security. On the actual day, a major seminar will be held at which the keynote speaker will be the Minister of Education, Tuula Haatainen. Adverts for the National Information Security Day will be published in the main newspapers, and the media will also be encouraged to get involved in the information security debate well before the day itself. Information on the content and aims of the event was widely circulated in autumn 2004, and various press briefings and media events have been organized. It is hoped that the media will produce articles and news items on information security and on the National Information Security Day, both on the day and afterwards.

For the general public, a key source on information security is the website opened last spring (www.tietoturvaopas.fi), which is continuously updated. The tietoturvakoulu.fi web service opened in November is also accessible to everyone.

The publicity and advertising material for the National Information Security Day will emphasize the following three principal messages:

Protect your computer

Every computer with an Internet connection should have an operating system with the latest information security updates, current anti-virus software and a firewall. You should also be careful about what material you download from the Internet. Taking backup copies of all important documents is also essential.

Make yourself secure

Privacy protection on the Internet cannot be taken for granted. You should carefully consider who you give your personal details to and who you chat with. Not everything is nice or true on the Internet.

Follow the rules

The same laws apply on the Internet as in normal life. A crime is always a crime, even in a computer network. Besides the law, you should also follow normal rules of good behaviour on the Internet.

Jussi Honkanen

Save the Children Finland

Heikki Huhtiniemi

Office of the Data Protection
Ombudsman

Eija Kara

Office of the Data Protection
Ombudsman

Marjatta Kuitunen

TeliaSonera Finland Oyj

Riikka Laitala

Song Networks Oyj

Tuula Laksola

Elisa Corporation

Riitta Luhtala

Helsinki Televisio Oy

Hannu Markus

Nokia Group

Jussi Matikainen

Helsinki City Education Department

Erkki Mustonen

F-Secure Corporation

Päivi Mutanen-Pirttilä

Information Society Programme

Heikki Mäenpää

Municipality of Kangasala

Pasi Mäki

Song Networks Oyj

Tapio Niemi

Municipality of Kangasala

Terhi Nikkilä

Song Networks Oyj

Kari Oksanen

Nordea Bank Finland Ltd

Mari Peltonen

Elisa Corporation

Suvi Rintala

Municipality of Kangasala

Mauri Rosendahl

Tietoturva ry

Olli Salminen

Finnish Information Society
Development Centre (TIEKE)

Riittamaija Stähle

The Finnet Association

Markku Suvanen

Ministry of Education

Project participants and project costs

The costs of the *National Information Security Day 2005* project will be about EUR 250,000.

This comprises the salary and other employment-related costs of the project coordinator, the creation of the www.tietoturvakoulu.fi web service, maintenance of the www.tietoturvaopas.fi website, publicity costs, marketing costs and the distribution of teaching materials to schools.

The companies and organizations marked with a red dot are each making a contribution of EUR 20,000 to the project costs or providing advertising space for the project under a separate agreement. All the companies and organizations listed have been involved in the work input on the project. In addition, the Finnish Federation for Communications and Teleinformatics (FiCom ry) is in charge of the project's financial management.

National Information Security Day 2005 is organized by

- Elisa Corporation
- The Finnet Association
- F-Secure Corporation
- Hewlett-Packard Oy
- Helsinki Televisio Oy
- Microsoft Oy
- Municipality of Kangasala
- Ministry of Transport and Communications
- The Mannerheim League for Child Welfare
- Save the Children Finland
- Nokia Group
- Nordea Bank Finland Ltd
- Finnish National Board of Education
- Ministry of Education
- Song Networks Oyj
- Association of Finnish Local and Regional Authorities
- TeliaSonera Finland Oyj
- Finnish Information Society Development Centre (TIEKE)
- Finnish Federation for Communications and Teleinformatics (FiCom ry)
- Office of the Data Protection Ombudsman
- Tietoturva ry
- Information Society Programme
- Finnish Communications Regulatory Authority (FICORA)

Impact and modifications

According to research by Taloustutkimus Oy (Internet Tracking) and Statistics Finland (on the use of communications tools and on-line shopping), National Information Security Day 2004 was a great success in that it increased ordinary Internet users' awareness of the hidden threats to information security and the means to avoid them. The forthcoming National Information Security Day 2005 has every chance of being at least as successful. It is hoped that the project will increase the information security awareness of the general public, and particularly that of schoolchildren.

In 2004, it was provisionally decided that the following Advisory Board projects would act as supporting projects for National Information Security Day 2005: 2.2. (Corporate information security awareness), 5.1. (Charting and developing information security awareness and competence) and 5.2. (Improving people's information security awareness). Project 5.2., in particular, will be well covered during the National Information Security Day. The 2005 event is

Anne Tamminen-Dahlman
Office of the Data Protection
Ombudsman

Kati Tuurala
Microsoft Oy

Satu Tyry-Salo
Association of Finnish Local and
Regional Authorities

Maritta Viljanen
Hewlett Packard Oy

being organized in exactly the same way as in 2004, with the exception that the household distribution of the printed leaflet on information security for home PC users undertaken in 2004 will not be repeated in 2005. The extent of advertising and publicity undertaken in 2005 (including customer communications by the project participants) will be at least as great as in 2004. It is therefore anticipated that a very high proportion of Finns will be aware of the messages contained in National Information Security Day 2005. The people managing this project have worked closely with those in charge of the 2.2. and 5.1. projects; project 5.1. will help ensure that the improvement in people's information security awareness continues to be monitored statistically in the future.

The National Information Security Day is an expensive project entailing a considerable amount of work for its organizers. The issue of who the project should belong to has also been debated, and a working group has considered the possibility of placing the project within the state administrative apparatus in the future, for example under the Finnish Communications Regulatory Authority (FICORA). How the project costs are met and how the work is divided are also areas that will need further examination in the future. The total amount of VAT on the services purchased for National Information Security Day 2005 over the duration of the project period will alone amount to approximately EUR 40,000.

Actors in the Finnish Information Security Sector

1. Aarnio Reijo, Office of the Data Protection Ombudsman
2. Ahola Ilkka, Sun Microsystems Oy
3. Ailisto Heikki, Technical Research Centre of Finland (VTT)
4. Andersson Martin,
Finnish Communications Regulatory Authority (FICORA)
5. Antikainen Päivi, Ministry of Transport and Communications
6. Anttila Johanna, Ministry of Transport and Communications
7. Arnell Jani,
Finnish Communications Regulatory Authority (FICORA)
8. Arnkil Lars, VR-Group Ltd
9. Arnö Kaj, MySQL AB
10. Aromaa Juha, The Mannerheim League for Child Welfare
11. Autio Jussi, The Finnet Association
12. Bergius Kimmo, Microsoft Finland Oy
13. Bonnici Keith, National Technology Agency of Finland (Tekes)
14. Elers Nora, Finnish Federation for Communications and
Teleinformatics (FiCom ry)
15. Haapaniemi Leena, SFS-Inspecta Certification
16. Hagman Rauni,
Finnish Communications Regulatory Authority (FICORA)
17. Hakola Tuomo, Ficix
18. Halkola Tapio, The Finnet Association
19. Halmelahti Joni, Federation of Finnish Enterprises
20. Hanski Mikko-Pekka, Idean Research Ltd.
21. Harald Bo, Nordea Bank Finland Ltd
22. Harjuhahto-Madetoja Katrina, Information Society Programme
23. Heinonen Arsi,
Finnish Communications Regulatory Authority (FICORA)
24. Heinonen Marja, Ministry of Transport and Communications
25. Heliö Erkki, TietoEnator Oy
26. Helkamäki Tarja, Elisa Corporation
27. Helopuro Sanna, Ministry of Transport and Communications
28. Herranen Mari, Ministry of Transport and Communications
29. Hiidenheimo Ilkka, Stonesoft Corporation
30. Holopainen Sami, Elisa Corporation
31. Honkanen Jussi, Save the Children Finland
32. Huhanantti Hellevi, Population Register Centre
33. Huhtiniemi Heikki, Office of the Data Protection Ombudsman
34. Huopio Kauto,
Finnish Communications Regulatory Authority (FICORA)
35. Hyppönen Ari, F-Secure Corporation
36. Hyvärinen Pertti, The Finnish Defence Forces
37. Hyytiä Kalevi, The Finnish Defence Forces
38. Härkönen Juha, Fortum Corporation
39. Ilmonen Urho, Nokia Group
40. Immonen-Oikkonen Pirjo, National Board of Education
41. Junnila Esko, Digita Oy
42. Jäppinen Arvo, Ministry of Education
43. Järvinen Antti, Kesko Corporation
44. Kaila Urpo, The Finnish IT Center for Science (CSC)
45. Kajantie Sari, National Bureau of Investigation
46. Kalinen Riku, Finnish Security Police
47. Kallio Jani, Elisa Corporation
48. Kananen Ilkka, National Emergency Supply Agency
49. Kara Eija, Office of the Data Protection Ombudsman
50. Kari Hannu H., Helsinki University of Technology
51. Karjalainen Jorma, Ministry of Finance
52. Karpinen Lauri, Office of the Data Protection Ombudsman
53. Karvonen Kaarlo, Finnair Plc
54. Keinälä Severi, Confederation of Finnish Industries (EK)
55. Kekkonen Timo, Ministry of Trade and Industry
56. Keronen Jouni, Fortum Corporation
57. Keskitalo Kari, Ministry of Trade and Industry
58. Kilkkilä Sami,
Finnish Communications Regulatory Authority (FICORA)
59. Kivi Ritva, National Board of Education
60. Kivinen Tuomas, Nordea Bank Finland Ltd
61. Kiviniemi Mikael, Ministry of Finance
62. Klemetti Kristiina, Finnish Federation for
Communications and Teleinformatics (FiCom ry)
63. Koivunen Erka, Elisa Corporation
64. Kokko-Herrala Riitta, Consumer Agency
65. Koli Markku, The Finnish Defence Forces
66. Korvola Kaarlo, Ministry of the Interior
67. Koskinen Sami O, Helsinki University of Technology
68. Krogars Marco, Ministry of Defence
69. Kuikka Suvi, Save the Children Finland
70. Kuitunen Marjatta, TeliaSonera Finland Oyj
71. Kuitunen Tero, Ministry of Trade and Industry
72. Kuparinen Veli-Pekka, National Emergency Supply Agency
73. Kyrölä Tuija, Helsinki Chamber of Commerce
74. Lahti Juhani, Song Networks Oyj
75. Laitala Riikka, Song Networks Oyj
76. Laksola Tuula, Elisa Corporation
77. Lantto Eeva,
Finnish Communications Regulatory Authority (FICORA)
78. Lappi Jaana, Ministry of Trade and Industry
79. Lauttamus-Kauppila Anna,
Finnish Communications Regulatory Authority (FICORA)
80. Lavonen Maria, SSH Communications Security Corporation
81. Lehtimäki Timo,
Finnish Communications Regulatory Authority (FICORA)
82. Lehtinen Kari, Elisa Corporation
83. Lehtonen Sami, Technical Research Centre of Finland (VTT)
84. Lepinsalo-Harju Elise, Nokia Group

85. Lillberg Petri, SSH Communications Security Corporation
86. Linnainmaa Leena, The Central Chamber of Commerce
87. Luhtakanta Perttu, The Finnish Defence Forces
88. Luhtala Riitta, Helsinki Televisio Oy
89. Luhtanen Leena, Minister of Transport and Communications
90. Malkki Merja, Finnish Federation for Communications and Teleinformatics (FiCom ry)
91. Markus Hannu, Nokia Group
92. Matikainen Jussi, City of Helsinki, Education Department
93. Mehtälä Martti, Microsoft Oy
94. Mellin Jorma, Ficix
95. Mellin Terttu, Ministry of Finance
96. Miettinen Kirsi, Ministry of Transport and Communications
97. Moilanen Usko, National Bureau of Investigation
98. Mustonen Erkki, F-Secure Corporation
99. Mutanen-Pirttilä Päivi, Information Society Programme
100. Mäenpää Heikki, Municipality of Kangasala
101. Mäenpää Markku, National Archives
102. Mäki Pasi, Song Networks Oyj
103. Naulapää Reijo, Ministry of the Interior
104. Niemi Tapio, Municipality of Kangasala
105. Nikkilä Terhi, Song Networks Oyj
106. Nurmela Juha, Statistics Finland
107. Nurmi Tiina, National Technology Agency of Finland (Tekes)
108. Ojajärvi Miina, Consumer Agency
109. Oksanen Kari, Nordea Bank Finland Ltd
110. Ovaska Anita, Elisa Corporation
111. Paananen Antti, Energy Market Authority
112. Palomäki Pirkka, F-Secure Corporation
113. Parmes Rauli, Ministry of Transport and Communications
114. Partanen Heikki, Office of the Data Protection Ombudsman
115. Peltonen Mari, Elisa Corporation
116. Perttula Juha, Ministry of Transport and Communications
117. Pietikäinen Kristiina, Ministry of Transport and Communications
118. Pitkänen Olli,
Helsinki Institute for Information Technology (HIIT)
119. Pohjola Hannele, Confederation of Finnish Industries (EK)
120. Porthan Juhani, Ministry of the Interior
121. Puhakainen Petri, Laurea Polytechnic
122. Purhonen Mika, National Emergency Supply Agency
123. Pursiainen Harri, Ministry of Transport and Communications
124. Rakshit Tommi, Ministry of the Interior
125. Rintala Suvi, Municipality of Kangasala
126. Rintanen Terho, The Finnish Defence Forces
127. Ristikankare Timo, Fingrid
128. Ristola Juhapekka, Ministry of Transport and Communications
129. Rosendahl Mauri, Tietoturva ry
130. Rostedt Nils, Oy LM Ericsson Ab
131. Saapunki Ari, Aldata Solution Finland Oy
132. Saaripuu Tuire, Population Register Centre
133. Saastamoinen Pentti,
Finnish Information Processing Association
134. Salmela Sari,
Finnish Communications Regulatory Authority (FICORA)
135. Salminen Helvi, Setec Oy
136. Salminen Olli,
Finnish Information Society Development Centre (TIEKE)
137. Saxén Timo, TeliaSonera Finland Oyj
138. Siilasmaa Risto, F-Secure Corporation
139. Simell Timo,
Finnish Information Society Development Centre (TIEKE)
140. Sirkä Jaana, F-Secure Corporation
141. Sivonen Hannu, National Emergency Supply Agency
142. Stähle Riittamaija, The Finnet Association
143. Suhonen Mari, The Finnish Terminology Centre (TSK)
144. Summanen Kari, National Board of Patents and Registration
145. Suvanen Markku, Ministry of Education
146. Svento Reijo, Finnish Federation for Communications and Teleinformatics (FiCom ry)
147. Tamminen-Dahlman Anne,
Office of the Data Protection Ombudsman
148. Tanner Simo,
Association of Finnish Local and Regional Authorities
149. Tarvainen Tapani, EFFI ry
150. Tassberg Antti, Nokia Group
151. Terho Arja, Ministry of Finance
152. Tiihonen Kalevi, Confederation of Finnish Industries (EK)
153. Tikkanen Leena, Centre for Metrology and Accreditation
154. Tuurala Kati, Microsoft Oy
155. Tyry-Salo Satu,
Association of Finnish Local and Regional Authorities
156. Vainio Arto, SSH Communications Security Corporation
157. Vettenranta Leena, Ministry of Justice
158. Viitasaari Mikko, TeliaSonera Finland Oyj
159. Viljanen Maritta, Hewlett-Packard Oy
160. Wilska Marita, Consumer Agency
161. Virkkunen Lauri, Vattenfall Oy
162. Virkkunen Tapio, Ministry of Transport and Communications
163. Wirman Kari, Elisa Corporation
164. Virtanen Teemupekka, Helsinki University of Technology
165. Vuorenmaa Ilkka, Anti-Piracy Centre in Finland
166. Vuorio Tiina, Microsoft Oy
167. Ylitalo Timo, The Finnish Bankers' Association
168. Zilliacus Stefan, Symantec Finland

Ministry of Transport and Communications

PO Box 31

00023 Government

Finland

Tel. +358 9 16002

www.mintc.fi