SAINT

The Finnish Regulator FICORA A Cybersecurity Reference Model

By Latif Ladid, IPv6 Forum President

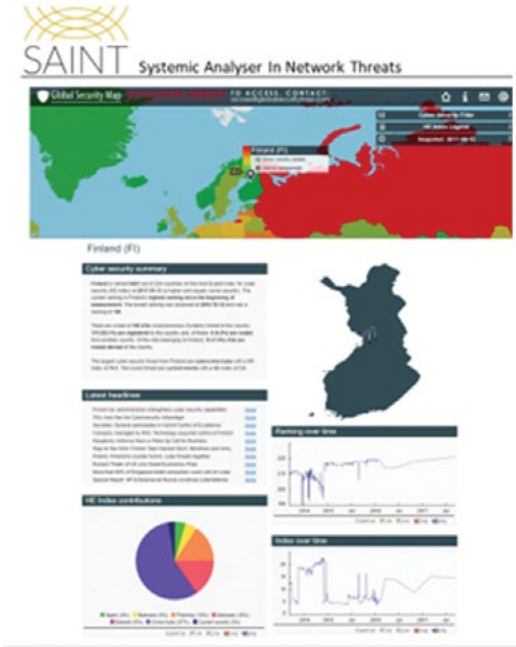
Latif Ladid, IPv6 Forum President

From SAINT's own findings, Finland ranks as one the most cybersecure nations in the world with a host exploit of just 14.3 from a scale of 1000 and ranks 221 country among the 224 countries investigated (Note: lower the number = higher the cyber threats mitigation).

The most important reason for this highly positive model is that the Finnish Communications Regulatory Authority (FICORA), as a regulator, is the prime interface for cybersecurity empowering it to issue direct instructions to the ISPs and cooperates with industry to achieve the same level of service, a Cybersecurity as a service (CaaS)

The second important vehicle is that the ISPs are empowered by the Finnish legislation to take actions, such as for example automatic prevention or limitation of message transmission or reception, in order to safeguard information security of their networks and services. This helps in directly stopping hacking of hostings and individuals.

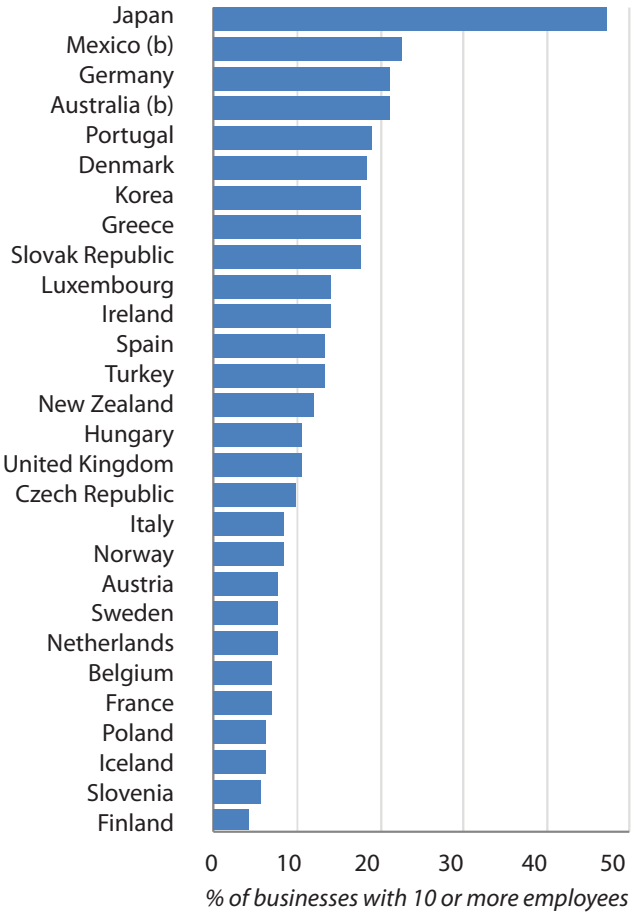
Fig.1 SAINT globalsecuritymap.com



Another viewpoint from OECD shows Finland as the lowest on a scale of businesses that have encountered IT security problems.

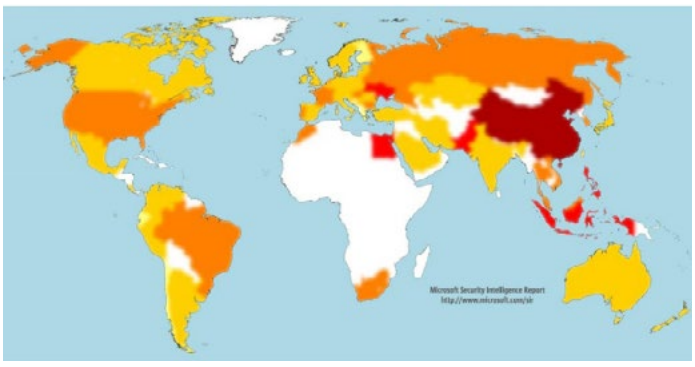
Fig. 2 OECD 2010

Businesses that have encountered IT security problems, 2010



From Microsoft SIR, March 2017: Locations with low concentrations of malware hosting sites included Finland (4.1), Taiwan (5.3), and Turkey (5.3).

Fig. 3 MS SIR 2017



Malware hosting sites PER 1,000 internet hosts, March 2017

20+ 15-20 10-15
5-10 > 0-5 insufficient data

FICORA boldly monitors and promotes communications markets and services, in the interests of the general public, business and industry. FICORA ensures that everyone has access to versatile, effective and secure communications in Finland.

The authority's activities contribute to a reliable information society and secure the status and rights of users of communications services by ensuring that society, business and citizens have access to, for example:

- fast and reliable telecommunications connections
- effective communications markets
- efficiently-used radio frequencies, numbers and codes
- reasonably-priced communications services of good quality
- versatile electronic media services; and
- objective information on the development, pricing and service level of communications markets and services.

FICORA maintains an overview of the functionality of electronic communications networks and information security, and reports of eventual information security threats. Also, the objective is to increase the awareness of information security in homes and companies for example by means of guidelines. FICORA also ensures the compatibility of communications networks and services.

The centralized administration of radio frequencies ensures that frequencies are used in as effective and disturbance-free manner as possible. This responsibility is significant both at national and international level.

FICORA supervises the .fi domain name registrars' technical information security and maintains the fi-domain name register. FICORA also grants telecoms operators the numbers and codes they need. This ensures that numbers are equally accessible to all telecoms operators, that there are enough numbers available and that the numbers are uniform.

Also, the authority enhances the provision of versatile electronic media services. FICORA

- collects licence fees;
- grants programming licences for TV and radio;
- monitors the content and advertising of TV and radio programmes; and
- monitors the functionality and service level of universal broadband, telephone and postal services;
- handles undeliverable postal items.

The Finnish Communications Regulatory Authority (FICORA) functions under the Ministry of Transport and Communications Finland.

FICORA is responsible for steering and supervising communication networks and services together with other operators in the field. The aim is to ensure that new service providers can enter the market, there is sufficient spectrum for new needs, and consumer rights are respected. FICORA provides government services related to information security for citizens, businesses and the public administration.

FICORA develops and monitors the operational reliability and security of communications networks and

services. It produces and publishes situational awareness of cyber security and acts as the National Communications Security Authority.

Information security services of the NCSC-FI
The National Cyber Security Centre Finland (NCSC-FI) at FICORA has been in operation since 1 January 2014. CERT (Computer Emergency Response Team Finland), NCSA (National Commuinications Security Authority Finland) and NRA (National Regulatory Authority) duties are part of the NCSC-FI's information security services. To support its operations, the NCSC-FI also maintains nationwide situational awareness of cyber security.

The NCSC-FI is a national information security authority. It develops and monitors the operational reliability and security of communications networks and services.

Its CERT duties consist of preventing, detecting and resolving security breaches, as well as of informing of information security threats. The Centre's NCSA duties include the responsibility for security matters related to electronic transfer and processing of classified information. The NRA duties aim to safeguard via guidance and supervision the confidentiality of electronic communication as well as operation and information security of Finnish networks and services.

The Centre's operations aim at ensuring that public communications networks and communications services are safe and interference-free, as well as securing critical societal functions. In accordance with the agreement entered with the National Emergency Supply Agency (NESA), the NCSC-FI is, for its part, responsible for ensuring the functionality of technical systems critical to the security of supply. The NCSC-FI wants to develop and diversify its information security services by means of e.g. development work and extensive partnership networks.

The English name National Cyber Security Centre Finland is intended for international use. In Finnish and Swedish, the Centre is called Kyberturvallisuuskeskus and Cybersäkerhetscentret respectively. The operational names CERT-FI and NCSA-FI are used in international stakeholder cooperation in accordance with established practice.

National Communications Security Authority, NCSA-FI
FICORA's NCSA-FI duties have been merged into the National Cyber Security Centre Finland (NCSC-FI). It specialises in information assurance matters related to the handling of classified information in electronic communications.
In Finland, several different authorities are responsible for our international obligations concerning information security. NCSA-FI operating within the National Cyber Security Centre Finland (NCSC-FI) is a part of the Finnish national security authority organisation.

Authorities responsible for information security

NCSA-FI's duties concerning international information security obligations:

- preparation of guidance and agreements concerning national security activities;
- preparation of guidance and agreements concerning national security activities;
- preparation of guidance on the handling of international classified information;
- management and accounting of the crypto material distribution network and guidance on the secure handling of the material (CDA);
- approval of cryptographic products for protecting international classified information in Finland (CAA);
- accreditation of information systems used for processing international classified information (SAA) (The accreditation process concerns government systems that are related to fulfilling international information security obligations and the systems of companies that participate in international competitive bidding and need accreditation from a National Communications Security Authority.);
- co-ordination of and guidance on national TEMPEST activities (NTA).

National Regulatory Authority, NRA
FICORA also has several duties concerning national information security obligations:

- steering and supervision of telecoms operators' operations, information security and preparedness: for example, monitoring compliance with the information security regulation (regulation no 67);
- steering and supervision of strong electronic identification and the provision of qualified certificates: for example, monitoring compliance with regulation no 72 issued by FICORA and carrying out annual audits of certification authorities providing qualified certificates;
- CERT-FI

FICORA's CERT-FI duties have been merged into the National Cyber Security Centre Finland (NCSC-FI).
The duties of CERT-FI include:

- solving information security violations and threats against network, communications and value-added services;
- gathering information on such incidents;
- disseminating information on information security matters.

The objective of CERT-FI's activities is to:

- ensure that public communications networks and communications services function safely and properly;
- safeguard functions that are vital to society.

Targets and methods for steering and supervision
FICORA steers and supervises compliance with the provisions and regulations that apply to its field of activity. FICORA's steering and supervision applies to telecommunications operators, TV and radio operators, users of radio frequencies, postal operators, and other several players related to electronic communications networks.

The matters of interpretation often concern how to

define telecommunications and a telecommunications operator or other conveyance of communications. The last-mentioned is supervised by FICORA as of the beginning of 2015. FICORA does not supervise the content or marketing of communications. FICORA is in favour of preventive and extensive measures and also aims at improving the operational possibilities of companies.

Players subject to FICORA's regulation

The legislation supervised by FICORA concerns, among others:

- traditional telecommunications operators - also in television and radio networks (telecommunications)
- several commercial and non-commercial providers of communications networks and communications services which have not traditionally been perceived as telecommunications operators (telecommunications)
- corporate or association customers that process their customers' identification data (corporate or association subscriber)
- as of 1 January 2015, also other parties than telecommunications operators and corporate or association subscribers that convey electronic communications as a third party with regard to the parties to the communications (other communications provider)
- housing companies and other holders of internal communications networks in real estate buildings
- telecommunications and antenna contractors that install internal networks to real estate buildings
- public authority networks
- providers of directory inquiry services
- providers of electronic remote controls (information society services)
- users of radio frequencies
- manufactures of radio and telecommunications terminal equipment and network equipment, importers, retailers, and inspection bodies
- providers of a qualified certificate
- providers of strong electronic identification
- authorities responsible for authorities' information systems and telecommunications arrangements and companies that implement them
- authorities and companies that process international classified information
- inspection bodies of the information security of information systems and telecommunications arrangements
- postal operators, particularly universal postal service

The legislation supervised by FICORA does not concern the content of communications at all, for example the content provided on the internet. However, requirements concerning the programme content have been imposed

- on television and radio operators (television and radio operations), and
- on providers of Video-on-Demand (VoD) services.

Further information on the interpretation of telecommunications

Proactive supervision

Examples of proactive supervision are

- planning of radio frequencies, and related international and national stakeholder cooperation
- drafting regulations specifying obligations in the legislation
- imposing universal service obligations and obligations based on significant market power on telecommunications operators
- drafting guidelines, recommendations and interpretation principles
- sectoral working groups and other national stakeholder cooperation
- drafting clarifications and reports
- producing information concerning the sector and other monitoring of the development in the sector

The goals of FICORA's supervision

The goal is to

- recognise problems in time and prevent them
- settle matters in cooperation with players, but by ensuring the confidentiality of the information
- act in such a manner that the effects of the measures are as effective as possible and apply to a large group
- act flexibly in such a manner that unnecessary litigations are avoided
- invest in steering and supervision of basic services
- issue, always when necessary, a written decision which may be appealed to an administrative court.

Operators' rights and obligations

Communications providers, such as telecommunications operators, have the obligation to ensure that the information security of their network and communications services is not compromised. Ensuring information security may require measures that affect customers' communications.

The Finnish legislation states that a telecoms operator must maintain the information security of its network and communications services by ensuring:

- operating security
- communications security
- hardware and software security
- data security.

Operators are not required to take unreasonable measures for ensuring information security as long as the measures are commensurate with:

- the seriousness of threats
- the level of technical development
- the costs.

In order to prevent information security violations and to ensure information security, a telecoms operator has the right to:

- prevent the conveyance and reception of messages
- remove from messages malware that pose a threat to information security
- take any other comparable technical measures in its communications network.

An operator may undertake these measures only if they are necessary for safeguarding the network or communications services or the communications ability of a message recipient. The measures taken to ensure information security may not limit freedom of speech or the protection of privacy any more than is necessary.

A telecoms operator must immediately notify its customers and FICORA of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes communication services.

A telecoms operator also has to notify its customers of:

- measures available to customers for protecting themselves against the information security threats discovered identified and the costs of such measures
- sources of further information on the threats.

Conclusion

From SAINT's own findings, it is abundantly clear that Finland has empowered itself with Cybersecurity legislation, partnership with ISPs and industry with tools and resources to reach the top rank as one the most cybersecure nations in the world

The most important reason for this highly positive model is that the Finnish Communications Regulatory Authority (FICORA), as a regulator, is the prime interface for cybersecurity empowering it to issue direct instructions to the ISPs and cooperates with industry to achieve the same level of service, a Cybersecurity as a service (CaaS)

The second important vehicle is that the ISPs are empowered by the Finnish legislation to take actions, such as for example automatic prevention or limitation of message transmission or reception, to safeguard information security of their networks and services. This helps in directly stopping hacking of hostings and individuals.

From the SAINT's project point of view, the Finnish model is to serve the EU member States and Associates states and probably worldwide as the most effective model to garner support and get strong consensus among all key stakeholders to fence off the dramatic onslaught of Cybersecurity threats in the end of this decade and the next one.

Acknowledgement: "The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 740829 - SAINT project."

Consortium members of the SAINT project.