OECD Organisation for Economic Co-operation and Development

Security of Information Systems and Networks

Security must become an integral part of the daily routine of individuals, businesses and governments in their use of Information and Communication Technologies (ICTs) and conduct of online activities.

SECURITY IS KEY TO USERS' TRUST IN E-BUSINESS AND E-GOVERNMENT.

Surveys show that security risks hinder the growth of online activities.

SECURITY IS THE ACHILLE'S HEEL OF THE DIGITAL SOCIETY.

As economic and social activities are increasingly conducted through interconnected systems and networks, the security of these systems and networks becomes critical.

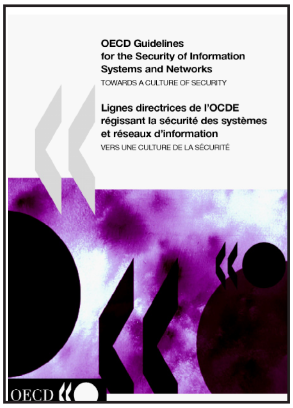
SECURITY IS AN INTERNATIONAL POLICY CHALLENGE.

In globally interconnected societies, security of information systems and networks is as strong as the weakest link. Furthermore, viruses, like other digital security threats, do not stop at the borders. International dialogue and co-ordination among governments and with other stakeholders are essential to design and implement national policies that are effective in an international environment.

OECD Security Guidelines

▶ The "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (2002) aim to promote security in the design and use of ICTs through:

- Guiding the development of effective national policies to address security threats and vulnerabilities in a global interconnected society, while preserving important societal values such as privacy and individual freedom.
- Developing a "Culture of Security" across society, so that security becomes an integral part of the daily routine of individuals, businesses, and governments in their use of ICTs and conduct of online activities.
- Encouraging each participant to become aware of risks, assume responsibility and take steps to enhance the security of information systems and networks while respecting ethical values.
- Providing a clear reference framework based on 9 principles at policy and operational levels.
- Benefiting the broader international community: the United Nations, the Council of the European Union, APEC and ASEM have all recognised or used the Guidelines.



OECD Guidelines for the Security of Information Systems and Networks
TOWARDS A CULTURE OF SECURITY
Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information
VERS UNE CULTURE DE LA SÉCURITÉ
OECD

9 principles

- Awareness
- Responsibility
- Response
- Ethics
- Democracy
- Risk Assessment
- Security Design & Implementation
- Security Management
- Reassessment

▶ The "Promotion of a Culture of Security for Information Systems and Networks in OECD Countries" (2005) is a unique resource on government action in 18 OECD countries to implement the Security Guidelines, in particular regarding the focus of their national policies for information security, their approach to fighting cybercrime and protecting critical information infrastructures, the development of CERTs, awareness-raising and education initiatives, research and development, evaluation and assessment, outreach to SMEs, international co-operation, etc. Links to national and international initiatives to promote a culture of security can also be found in the OECD Culture of Security Web Site at *www.oecd.org/sti/cultureofsecurity*

www.oecd.org/sti/security-privacy

Ongoing OECD Work on Information Security

An evolving environment:

- **The Internet has become a critical infrastructure,**
- **societies and economies are converging on the Internet, and**
- **the distinction between physical and virtual worlds is blurring.**

▶ Critical Information Infrastructure Protection

The 2005 report on the Promotion of a Culture of Security in OECD Countries highlighted that an important focus for many government national implementation plans was on ensuring the resilience of critical information infrastructures (CII), whose protection may involve coordination beyond national borders. By analysing the drivers for and challenges to the development of CII security policies in a number of volunteer countries, the OECD helps governments to share experiences and practices on assessing and managing risks to CII, on the emerging and existing models for public-private information sharing and on national responses to the growing need for cross-border collaboration.

▶ Electronic Authentication

Providing assurance to a party regarding who or what that party is interacting with is a key requirement for trust in a digital environment. Electronic authentication fosters trust and helps reduce security risks. Building on work since 1998 aimed at enabling cross-jurisdictional interoperability of authentication, the OECD is finalising policy and practical guidance for electronic authentication to help countries in establishing their approaches to authentication and to facilitate cross-border exchanges.

▶ Malware and Identity Theft

Malicious software is used for extortion schemes targeting large and small businesses (e.g. via distributed denial of service attacks) and identity theft targeting individuals (e.g. via phishing scams) and, with armies of hundreds of thousands of zombie PCs called "botnets", it could also be used for other criminal purposes such as cyberterrorism. OECD work on malware, conducted in co-operation with the Asia-Pacific Economic Co-Operation (APEC), aims to provide governments with a holistic understanding of the phenomenon, taking into account its cross-border dimension. It will help them develop and implement coordinated policies for effectively fighting criminal malware-based activities, including identity theft, from the economic, technological, regulatory and educational fronts.

▶ Digital Identity Online

Identity management (IDM) holds the promise to help mitigate security risks which have been amplified by the trend towards broadband-enabled "anytime-anywhere" Internet access. However, protecting information in a complex (fixed, wireless, mobile), dynamic and interoperable computing environment raises security challenges related to the secure information sharing and dissemination as well as regarding confidentiality, integrity and availability of the information stored and maintained in an IDM system. The OECD will examine these challenges in the context of its broader work on IDM.

▶ RFID, sensors and pervasive networks

RFID tags, location devices and sensor devices can be invisible to individuals, hold the potential to become pervasive in the long term and, in combination with ubiquitous networks, could collect and process data everywhere, all the time. Considering this emerging trend, the OECD is exploring the applicability of the OECD Privacy Guidelines and Security Guidelines in such environments.

For more information: OECD Working Party on Information Security and Privacy Secretariat
OECD – DSTI – ICCP – 2, rue André Pascal – 75775 Paris Cedex 16 – France
Tel: +33 (0) 1 45 24 82 00 – Fax: +33 (0) 1 44 30 62 59 – email: dsti.contact@oecd.org

www.oecd.org/sti/security-privacy