

INFORMATION TECHNOLOGY AND SECURITY

Strengthening security and trust

Security and trust are crucial to developing a digital economy. Enhancing the security of information systems and networks, as well as building trust in global communications networks, remain key policy challenges for furthering the development of information and communications technology (ICT), and economic growth. As research and surveys show, a lack of security and trust online is likely to have a negative impact on the emerging digital economy. Security and trust in ICT have a central place in the OECD's vision of a global digital economy and the potential it holds for economic growth, better living standards and improved social conditions. User trust in the information society and in global networks hinges on assuring consumers and businesses that their use of network services is secure, reliable and verifiable. The OECD has been working in the area of trust since the infancy of the information economy, producing the Guidelines for Privacy Protection in 1980 and the Security Guidelines for Information Systems in 1992. Building security and trust in the digital economy raises policy challenges which call for the broad analysis and public-private sector dialogue for which the OECD is so well suited.

Strengthening information security so that it can stand up to both internal vulnerabilities and external threats such as cyber-terrorism, computer viruses or hacking is key to securing trust in global networks and to protecting critical infrastructures. The revised OECD Guidelines for the Security of Information Systems and Networks ("Security Guidelines", 2002) go beyond raising public awareness of the risks to information systems and networks, and offer advice on the policies, practices, measures and procedures available to address those risks, while emphasising the need for the adoption and implementation of the Guidelines. They call for all stakeholders (governments, businesses and end users) to develop a "global culture of security". In short, the aim is to foster greater trust and confidence in information systems and networks, and in the ways in which they are delivered and used.

Shared risks, shared responsibilities

In a global networked environment, risks, threats and responsibility are shared. All participants – governments, businesses and end users – have experienced the virus and worm attacks that have rapidly spread across the world. The dramatic recent increase in spam (unsolicited e-mail) adds to existing security risks, as spam is used as a vehicle to spread malicious payload. Beyond technical solutions, strengthening information security calls for a change in risk perception and behaviour by all participants throughout society. Such a cultural change should balance the need for enhanced security with preserving respect for privacy and other important democratic values. The development of a culture of security is a collective responsibility; it should build trust in the global information society by ensuring the reliability, integrity and sustainable development of information

systems and networks. As the nature of the threats to information systems and networks is constantly changing, security of such systems requires an ongoing co-operative effort by all stakeholders, both nationally and internationally.

International support

The Security Guidelines, which are a response to the ever-changing security environment and which call for the creation of a culture of security, have received wide support at both national and international level. They served as the basis for a United Nations General Assembly resolution for the “Creation of a Global Culture of Cyber Security” in December 2002 (UN Resolution A/RES/57/239) and have been recognised by the Council of Ministers of the Asia Pacific Economic Co-operation (APEC) forum and the Council of the European Union.

Implementing security

OECD member countries are actively implementing the 2002 Security Guidelines. In January 2003, OECD countries adopted an implementation plan for co-ordinated national online security policies and undertook a survey to monitor progress in implementing the Guidelines. In October 2003, the Norwegian government hosted the OECD Global Forum on Information Systems and Network Security. The Forum aimed to share information with OECD members, non-members, the business community and civil society, and to enable a forward-looking discussion on expanding the culture of security. Stock was taken of progress made in the national implementation of the Security Guidelines.

A “Culture of Security” web site has been created to provide member and non-member governments with a tool for exchange of information on initiatives to implement the 2002 OECD Security Guidelines. The site provides access to relevant web sites as a first step towards creating a global culture of security; and with the aim of providing a centralised portal for educational security tools for users of information systems and networks.

Actions for the future

OECD member countries have already committed themselves to taking a leading role in strengthening information security. They have decided action-oriented initiatives to build an effective global culture of security. Indeed, drawing lessons from experience at national level, and exchanging practical and detailed information for ensuring information security is essential to enhancing national and global cyber-security. Building on information already gathered, member countries will be carrying out an in-depth inventory of national initiatives to implement the Security Guidelines with a view to assembling a critical mass of detailed information and case studies. This information will be shared among member and non-member economies.

Since spam has the potential to seriously undermine information security and trust, the OECD has decided to take action and help co-ordinate international co-operation to combat spam. Building on its work in 2003 and on the results of the OECD workshop on spam, hosted by the European Commission in February 2004, this action will aim at developing a consistent multi-pronged approach to fighting spam, including facilitating cross-border enforcement against spammers.

Outreach

Outreach to non-member economies is crucial for improving information security on the global scale. To be effective, a culture of security must be global and must involve

non-member economies, as the level of security in interconnected systems is only as good as the weakest link. Non-member economies are in the process of adopting a similar approach to that of OECD member countries, but have specific needs that should be addressed. Information sharing between OECD members and non-members on practical initiatives and experiences is particularly important. To this end, the OECD will continue to strengthen its efforts to co-operate with non-member economies within APEC and beyond, and will further contribute to the World Summit on the Information Society (WSIS) process, as appropriate.

Other essentials for trust

In addition to strengthening security of ICT, building trust in the digital economy requires appropriate privacy and consumer protection. Beyond security, the OECD continues to promote privacy and consumer protection as essential building blocks for trust.

Following up on previous work, the OECD adopted Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders in June 2003. The Guidelines set out broad principles for international co-operation and specific provisions covering notification, information sharing and assistance with investigations. They also cover issues regarding the authority of consumer protection enforcement agencies, invite private-sector co-operation, and set the stage for future work on consumer redress. Implementation of the Guidelines is a key work item.

Privacy Online: OECD Guidance on Policy and Practice has been updated and published in 2003. It is aimed at governments, businesses and individuals, and promotes privacy protection at national and the international level. *Privacy Online* outlines methods for adopting and posting a privacy policy, and proposes mechanisms for enforcement and redress, and ways to promote education and user awareness.