I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 131–135
IOS Press

In Focus

OECD Promotes Culture of Information Security

1. Introduction

Confirming concerns of its 30 member countries over exposure to risks and threats to information systems and networks, the OECD Council of Ministers in July 2002 adopted Guidelines for the Security of Information Systems and Networks. This was followed by an Implementation Plan issued in January 2003. The Guidelines "signal a clear break with a time when secure design and use of networks and systems were all too often afterthoughts". Due to the increasing dependence on information systems, networks and related services, OECD ministers agree, countries must establish a heightened priority for security planning and management in order to create an environment advance a "culture of security". The following are excerpts from the official text of the Guidelines.

2. Aims of the Guidelines

- Promote a culture of security among all participants as a means of protecting information systems and networks.
- Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
- Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
- Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- Promote cooperation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

3. Principles

A program of nine principles have been designed to be complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy.

1) *Awareness*

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks

ISSN 1084-4678/03/$8.00

under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) *Responsibility*

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) *Response*

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and cooperative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and cooperation.

4) *Ethics*

Participants should respect the legitimate interests of others.

Given the pervasiveness of information systems and networks in our societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others.

5) *Democracy*

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) *Risk assessment*

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) *Security design and implementation*

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and coordinated to optimize security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) *Security management*

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) *Reassessment*

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

4. Implementation Plan for the Guidelines

The OECD Working Party on Information Security and Privacy was assigned the responsibility to prepare an implementation plan for the Guidelines. In describing this plan, the Working Party stressed "the promotion of a culture of security will require not only leadership but also broad participation at all levels of government, business, and civil society to heighten the priority for security planning and management, as well as to increase understanding of the need for security among all participants. The Guidelines and related outreach campaigns should encourage participants to factor security into the design, implementation, and use of all information systems and networks".

Involvement of the private sector, the Working Party notes, is particularly important since it "designs, builds, owns and operates most of the infrastructure of information systems and networks". Business as well as other participants are encouraged to formulate their own initiatives to implement the Guidelines. Continued cooperation among government, business and civil society is also required in follow-up work on the Guidelines. Public-private partnerships offer a good platform for fostering such relationships.

5. Roles of Government

Government has a responsibility to provide leadership in developing a culture of security. It should provide this leadership in each of its roles related to information systems and networks that include the development of public policy, as owner and operator of systems and networks, and as a user of such systems and networks. In developing public policy, government should promote the security of information systems and networks to engender confidence in their use and better ensure economic growth and overall security. Public policy development is a unique role of government but one that should be carried out in a transparent fashion and in consultation with other participants and concerned parties. Of particular note in this regard is government's responsibility for education, training, and the provision of information resources to the public, an activity that also assists government in fulfilling its other roles. As owner and operator of information systems and networks, government shares a role with businesses and other organizations and has responsibilities to lead by example. As a user of information systems and networks government shares a role with businesses, other organizations, and individuals for ensuring use of the system and network consistent with a culture of security. The following sections look more closely at government's responsibilities and opportunities in these various roles.

A) Government responsibility for public policy

1. Develop national policy on information security and ensure cross-border cooperation to promote a global culture of security.

Government should recognize the increasing need for a comprehensive policy and institutional infrastructure to ensure public safety, security and economic well-being in response to the threats and vulnerabilities associated with globally interconnected information systems and networks. Governments are further encouraged to respond by establishing new or amend existing policy that may incorporate principles of the Guidelines. In doing so, principles in the Guidelines may need to be aligned with the national situation in

the area, and ongoing or planned national initiatives. Such initiatives may include policies to combat cyber crimes, such as:

- Enacting a comprehensive set of substantive criminal, procedural and mutual assistance legal measures to combat cybercrime and ensure cross-borders cooperation. These should be at least as comprehensive as, and consistent with, the Council of Europe Convention on Cybercrime (2001).
- Identifying national cybercrime units and international high-technology assistance points of contact and creating such capabilities to the extent they do not already exist; and
- Establishing institutions that exchange threat and vulnerability assessments (such as national CERTs (Computer Emergency Response Teams).

The development of these policies should be consistent with the Guidelines, in particular, the principles on ethics and democracy that provide the societal references for addressing security. These public policies should also be developed in conjunction with other participants (business, other organizations and users) to better ensure transparency and that the aims of the Guidelines' principles can be met in an effective manner.

2. Outreach and support for other participants

A second aspect of government's public policy role is to conduct outreach and support efforts by all participants to address security. In the first instance government action should raise awareness of law and policy that address cybersecurity. Beyond this, government should facilitate awareness and appropriate responses by other participants through programs and initiatives.

These efforts could include, but not be limited to, highlighting the nature of the problem, assisting participants to address their security responsibilities, supporting education and training, establishing points of contact and resource sites for practical information, and removing obstacles to action by participants. Government should also consider support for R&D, the development of best practices, and building partnerships among participants to address information security. As part of its public policy role, government can utilize its significant purchasing power and system/network size to support efforts to increase security through improved security in software, hardware, and best practices operational procedures. This public policy role also extends to addressing response to and recovery from cyber incidents.

Awareness raising can be achieved through consistently emphasizing the necessity of security at every opportunity. Education, training, press releases, Web sites, public announcements, offering tools and kits are among the current identified means to raise awareness. Government should continue to emphasize the importance of awareness of the risks and available safeguards to participants. Such awareness-raising campaigns should aim to ensure that participants become fully aware that:

- Information systems and networks can be affected by both internal and external risks.
- Security failures may significantly harm systems and networks both under and outside of their control.
- There is potential harm to and from others arising from interconnectivity and interdependency.
- It is important to understand the configuration of, and the availability of updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.
- They should adopt safeguards/solutions to deal with known threats and vulnerabilities.
- They should develop security goals that are appropriate to their needs in preventing, detecting and responding to threats and vulnerabilities.
- They should be accountable in a manner appropriate to their individual roles.
- They should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environments.

Examples of initiatives in this category can be found on the Web sites of several governments including at the US Federal Trade Commission: http://www.ftc.gov/bcp/conline/edcams/infosecurity/forkids.html.

Exchange of best practice should facilitate users' ability to better understand and achieve the goal of effective and up-to-date security measures.

In designing education and information programs, not only tips to ensure the security of the systems and networks are necessary, but also emphasis on the ethics to promote conduct that recognizes security needs and respects the legitimate interests of others. Government initiated education and outreach programs should also promote conduct that aims at ensuring security in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the

confidentiality of information and communication, the appropriate protection of personal information, openness and transparency. Assessing the impact of planned security measures on these values should also be encouraged.

Further efforts are necessary so that users of the systems and networks should know how to set up and maintain their systems and networks, be aware of the latest vulnerabilities, and know whether or not software patches are available. They should also know what to do when security incidents occur, including timely action for seeking help.

Further efforts are necessary for the development of information security educational programs wherever IT use is taught, such as in engineer education, health education or general computer education programs currently undertaken in schools and universities.

Information concerning useful sites such as those of CERT[1] or SANS[2] and various industry information sharing and analysis centers (ISAC) are well known. Further efforts are necessary to continue to support such initiatives to establish sources of practical information and publication of the references to such sources. Governments should encourage participants, especially business, to utilize, share and distribute useful information through such institutions.

B) Government as owner and operator of information systems and networks

Government must address the principles of risk assessment, security design and implementation, security management, and reassessment, just as any other owner and operator of information systems and networks. Government should develop policies that reflect best practices in security management and risk assessment. Security management should be based on a risk assessment that identifies threats and vulnerabilities and is sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Government's security management should also be dynamic, encompassing all levels of government's activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. And, these information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security. Internationally recognized information security management standards, such as ISO standards and industry-specific standards, may be used to establish an effective system of security management.

Because of the size of its operations, government has a special responsibility to become a model owner/operator and to lead by example. Government can thus use its operational expertise to facilitate the development of best practices and other operational improvements for the benefit of all participants. Government can also use its significant purchasing power in information systems and networks to encourage the development and expanded availability of more secure products and services.

C) Government as user of information systems and networks

As a user of information systems and networks, government has a responsibility to ensure that its use is consistent with the Guidelines, in particular the ethics and democracy principles, and thus contributes to a secure global system. Because individual government employees constitute government use, government must ensure its employees are aware of security concerns, their individual responsibilities and have the capability to respond in an appropriate way to security incidents. Development by government of an appropriate security environment, training, and tools will not only facilitate security on government systems and networks, but can also serve as foundation elements for government's outreach as a public policy matter.

[1] Computer Emergency Response Team, Carnegie-Mellon University (http://www.cert.org).

[2] SANS (SysAdmin, Audit, Network, Security) Institute. For example, in October 2002, SANS Institute and the FBI released a list summarizing the Twenty Most Critical Internet Security Vulnerabilities (http://www.sans.org/top20/).