GENERAL DISTRIBUTION

OCDE/GD(92)190

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Paris 1992

>

PREFACE

•Explosive growth in use of information systems for all manner of applications in all parts of life has made provision of proper security essential. Security of information systems is an international matter because the information systems themselves often cross national boundaries and the issues to which they give rise may most effectively be resolved by international consultation and co-operation.

•In 1990, the Information, Computer and Communications Policy (ICCP) Committee created a Group of Experts to prepare Guidelines for the Security of Information Systems. The Group of Experts included governmental delegates, scholars in the fields of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users. The Expert Group was chaired by the Hon. Michael Kirby, President of the Court of Appeal, Supreme Court of New South Wales, Australia. Ms. Deborah Hurley of the Information, Computer and Communications Policy Division of the OECD's Directorate for Science, Technology and Industry drafted the Recommendation, the Guidelines and the Explanatory Memorandum, based upon the deliberations of the Expert Group at its meetings.

•The Expert Group met six times over 20 months -- in January 1991, March 1991, September 1991, January 1992, June 1992 and September 1992 -- to prepare the Recommendation of the Council Concerning Guidelines for the Security of Information Systems, the Guidelines for the Security of Information Systems, and the Explanatory Memorandum to Accompany the Guidelines. The Group of Experts submitted the final version of the three texts to the ICCP Committee at its twenty-second session on 14-15 October 1992. The ICCP Committee approved the texts and their transmission to the Council of the OECD.

•On 26 November 1992, the Council of the OECD adopted the Recommendation of the Council Concerning Guidelines for the Security of Information Systems and the 24 OECD Member countries adopted the Guidelines for the Security of Information Systems.

CONTENTS

RECOMMENDATION OF THE COUNCIL

CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

26 November 1992

THE COUNCIL,

HAVING REGARD TO:

the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 (b), 1 (c), 3 (a) and 5 (b) thereof;

the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [C(85)139,Annex];

RECOGNISING:

the increasing use and value of computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance (all hereinafter referred to collectively as "information systems");

the international nature of information systems and their worldwide proliferation;

that the increasingly significant role of information systems and growing dependence on them in national and international economies and trade and in social, cultural and political life call for special efforts to foster confidence in information systems;

that, in the absence of appropriate safeguards, data and information in information systems acquire a distinct sensitivity and vulnerability, as compared with paper documents, due to risks arising from available means of unauthorised access, use, misappropriation, alteration, and destruction;

the need to raise awareness of risks to information systems and of the safeguards available to meet those risks;

that present measures, practices, procedures and institutions may not adequately meet the challenges posed by information systems and the concomitant need for clarity, predictability, certainty, and uniformity of rights and obligations, of enforcement of rights, and of recourse and redress for violation of rights relating to information systems and the security of information systems;

the desirability of greater international co-ordination and co-operation in meeting the challenges posed by information systems, the potential detrimental effects of a lack of co-ordination and co-operation on national and international economies and trade and on participation in social, cultural and political life, and the common interest in promoting the security of information systems;

AND FURTHER RECOGNISING:

that the Guidelines do not affect the sovereign rights of national governments in respect of national security and public order ("ordre public"), subject always to the requirements of national law;

that, in the particular case of federal countries, the observance of the Guidelines may be affected by the division of powers in the federation;

RECOMMENDS THAT MEMBER COUNTRIES:

1. establish measures, practices and procedures to reflect the principles concerning the security of information systems set forth in the Guidelines contained in the Annex to this Recommendation, which is an integral part hereof;

2. consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures for the security of information systems;

3. agree as expeditiously as possible on specific initiatives for the application of the Guidelines;

4. disseminate extensively the principles contained in the Guidelines;

5. review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems.

Annex to the Recommendation of the Council
of 26 November 1992

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

26 November 1992

I. AIMS

The Guidelines are intended:

-- To raise awareness of risks to information systems and of the safeguards available to meet those risks;

-- To create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems;

-- To promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures;

-- To foster confidence in information systems and the manner in which they are provided and used;

-- To facilitate development and use of information systems, nationally and internationally; and

-- To promote international co-operation in achieving security of information systems.

II. SCOPE

The Guidelines are addressed to the public and private sectors.

The Guidelines apply to all information systems.

The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.

III. DEFINITIONS

For the purposes of these Guidelines:

- -- "data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means;

- -- "information" is the meaning assigned to data by means of conventions applied to that data;

- -- "information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance;

- -- "availability" means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner;

- -- "confidentiality" means the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner;

- -- "integrity" means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

IV. SECURITY OBJECTIVE

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

V. PRINCIPLES

1. Accountability Principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

7. Timeliness Principle

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

VI. IMPLEMENTATION

Governments, the public sector and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative, self-regulatory and other measures, practices, procedures and institutions for the security of information systems. Where provision has not already been made, they should, in particular:

Policy Development

-- Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:

. harmonized worldwide technical standards, methods and codes of practice;

. promotion of expertise and best practice in the security of information systems;

. formation and validity of contracts and other documents created and executed in or by means of information systems;

. allocation of risks and liability for failures of the security of information systems;

. penal, administrative or other sanctions for misuse of information systems;

. jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies;

. mutual assistance, extradition and other international co-operation in matters relating to the security of information systems; and

. means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings.

Education and Training

-- Promote awareness of the necessity for and the goals of security of information systems, including:

. ethical conduct in the use of information systems; and
. adoption of good security practices.

-- Provide and foster education and training of:

. developers, owners, providers and users of information systems;
. specialists and auditors of information systems;
. specialists and auditors of security of information systems; and
. law enforcement authorities, investigators, attorneys and judges.

Enforcement and Redress

-- Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.

-- Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

Exchange of Information

-- Facilitate the exchange of information relating to the Guidelines and their implementation.

-- Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.

Co-operation

-- On national and international levels, consult, co-ordinate and co-operate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonize as completely as possible measures, practices and procedures for the security of information systems.

EXPLANATORY MEMORANDUM

to Accompany the Guidelines for
the Security of Information Systems

PREFACE

In October 1988, the Committee for Information, Computer and Communications Policy (ICCP) of the OECD approved the preparation by the OECD Secretariat of a study on the subject of security of information systems. The report, entitled {Information Network Security, }was submitted to the ICCP Committee in October 1989. Following review of the Secretariat document, the ICCP Committee endorsed the convocation of a meeting of experts to explore in greater depth the issues raised in the report.

Based upon the advice of the experts, the ICCP Committee, in March 1990, approved the creation of a Group of Experts to draft Guidelines for the Security of Information Systems. The Group of Experts included governmental delegates, scholars in the fields of law, mathematics and computer science, and representatives of the private sector, including computer and communication goods and services providers and users. The Group of Experts met six times between January 1991 and September 1992 to prepare the Recommendation of the Council concerning Guidelines for the Security of Information Systems, the Guidelines for the Security of Information Systems, and the Explanatory Memorandum to Accompany the Guidelines.

The OECD is well-positioned to play a central role in building awareness of the need for security of information systems and of measures that might be undertaken to meet that end. OECD membership encompasses North America, the Pacific region and Europe. The lion’s share of development and exploitation of information systems occurs in OECD Member countries. Through the ICCP Committee, the OECD provides direction and coalesces opinion at an early stage on issues related to information, computer and communications technologies and policies and their effects on society, with a view to raising awareness on an international level and assisting governments and the private sector as they undertake national deliberations.

The Guidelines for the Security of Information Systems are intended to provide a foundation from which countries and the private sector, acting singly and in concert, may construct a framework for security of information systems. The framework will include laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities. It is hoped that the Guidelines will serve as a benchmark against which governments, the public sector, the private sector and society may measure their progress.

CONTENTS

INTRODUCTION

•A computer, a computer program and data constitute basic elements of an information system. The computer may be connected by communication equipment and devices into a network with terminals or other computers or communication facilities. A network may be a private local area network (LAN), an extended private network, such as a wide area network (WAN) or global network, or an external communication link open to anyone with the technological means to gain access to it. Many networks are composed of a combination of internal and external links. Communication networks include data communication, telephone and facsimile. Other ancillary equipment, printers, for example, may be attached to the computer and communications hardware. The computer programs might include operating system and application software, which may be custom-designed or purchased ready-made. The software may be installed in the computer or stored on magnetic, optical or other media. Paper manuals and documentation support the operation, use and maintenance of the hardware and software. This entire structure is created for the purpose of storing, processing, retrieving and transmitting data and information. These various elements may be combined to form an information system.*

Expanding Uses and Benefits of Information Systems

The significance of computer and communications technologies, economically, socially and politically, is widely accepted. They are key technologies not only in their own right but also as conduits for and components of other goods, services and activities.

Recent years have witnessed:

-- proliferation of computers;

-- increase of computing power with simultaneous
• decrease in costs;

---

* The dynamism of information and communication technologies dictates that this description of information systems may serve only to give an indication of the present situation and that new technological developments will arise to augment the potentialities of information systems.

-- convergence of computer and communication technologies;

-- greater interconnectivity and inter-operability of computer and communication systems;

-- increasing decentralisation of computing and communication functions; and

-- growth of computer use to the point that, in many countries, every individual is an actual or potential user of computer and communication networks.

The global information society has arrived. It is borderless, unconstrained by distance or time. Our economies, politics and societies are based less on geography and physical infrastructure than previously, and increasingly on information system infrastructures.

Information systems benefit governments, international organisations, private enterprise and individuals. They have become integral to national and international security, trade, and financial activity. They are widely used by government administrations, fiscal authorities, business organisations and research institutions. They are critical to the provision of health care, energy, transport, and communications. Information systems may be used for trading, voting, learning and leisure. Expanded use of information systems offers possibilities of greater access to resources, experience, learning, and participation in cultural and civic life.

Dependency

Every person, enterprise and government is affected by information systems and has become dependent on their continued proper functioning. For example, increased use of information systems has wrought fundamental changes in internal organisational procedures and has altered the way that organisations interact. In the event of an information system failure, it may not be possible to continue present procedures without information systems nor practicable to return to former methods. There may not be sufficient paper records, staff skills or even numbers of staff to permit an organisation to continue to work as productively as it does with its information system in operation, and as effectively as its competitors. Consider, for example, the effect of information system failure on the functioning and efficiency of airlines, banks or securities exchanges.

Dependence on information systems is growing. Concomitant is a mounting need for confidence that they will continue to be available and to operate in the expected manner.

Vulnerability

As use of information systems has increased enormously, generating many benefits, it has, in its wake, created an ever larger gap between the need to protect systems and the degree of protection presently utilised. Society, including business, public services and individuals, has become very dependent on technologies that are not yet sufficiently dependable. All the uses of information systems identified above are vulnerable to attacks upon or failures of information systems. There are risks of loss from unauthorised access, use, misappropriation, modification or destruction of information systems, which may be caused accidentally or result from purposeful activity. Certain information systems, both public and private, such as those used in military or defence installations, nuclear power plants, hospitals, transport systems, and securities exchanges, offer fertile ground for anti-social behaviour or terrorism.

The developments identified above, proliferation of computers, increased computing power, interconnectivity, decentralisation, growth of networks and the number of users, while enhancing the utility of information systems, also increase system vulnerability. It may be harder to locate a system problem and its causes, to correct it in balance with other system functions and requirements, and to prevent its recurrence or the occurrence of other lapses. As systems decentralise and grow larger, it is important to keep account of their interdependent components, which, increasingly, may come from multiple vendors and sources. Moreover, the growing interconnectivity of network systems and use of external networks multiply points of possible information system failures. These externalities lie outside the direct control of the system operators and the rights and duties of the parties in the event of breaches may be unclear.

Technical change is uneven. It leaps ahead in some areas while lagging in others. Inability to adapt to and absorb technological developments at the same rate at which they occur, such as failure adequately to test or co-ordinate system changes, may lead to system problems. Technological developments may be implemented before all their ramifications and relations to existing technologies are understood. Unequal distribution of system capabilities may give some persons more control of and access to information systems than is intended or desirable. Increasing numbers of users have access to information systems, while, at the same time, they are decreasingly directly controlled by system owners or providers.

Failures of information systems may result in direct financial loss, such as loss of orders or payment, or in losses that are more indirect or perhaps less quantifiable by, for example, disclosure of information that is personal, important to national security, of competitive value, or otherwise sensitive or confidential.

The evolution of the law is not always in step with technological progress. It is sometimes insufficient at the national level and in a number of cases still undeveloped at the international level. Harmonization of legislation is an important goal to be actively pursued.

Building Confidence

Users must have confidence that information systems will operate as intended without unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be exploited to the extent possible and further growth and innovation may be inhibited. Access to secure networks and establishment of security standards have already emerged as general user requirements. Loss of confidence may stem equally from outright malfunction or from functioning that does not meet expectations. ••••

Uncertainties may be met and confidence fostered by building consensus about use of information systems. Accepted procedures and rules are needed to provide conditions to increase the reliability of information systems. Developers, operators and users of information systems deserve reassurance as to their rights and obligations, including responsibility for system failures. Clear, uniform, predictable rules should be in place to ease and encourage growth and exploitation of information systems.

The security of information systems is an international issue because information systems and the ability to use them frequently cross national boundaries. It is a problem that may be ameliorated by international co-operation. Indeed, given the disregard of information systems for geographical and jurisdictional boundaries, agreements are best promulgated and accepted on an international level.

Experience in other sectors involving new technologies with the potential for serious harm reveals a three-part challenge: developing and implementing the technology; providing for avoiding and meeting the failures of the technology; and gaining public support and approval of use of the technology. The air transport industry has been fairly successful in implementing safety techniques and requirements. They facilitate the smooth functioning of air transport and inspire public confidence. Similarly, the shipping industry has successfully used ship certification systems to rank safety of vessels. The field of biotechnology is now grappling to meet the requirements of permitting technological development and preventing harm from exploitation of the technology and subsequent loss of public support. For information and communication technologies, the goal of avoiding and meeting failures of the technology includes the additional task of preventing and handling actual or potential intrusions to information systems.

SECURITY OF INFORMATION SYSTEMS

Security of information systems is the protection of availability, confidentiality and integrity. Availability is the characteristic of information systems being accessible and usable on a timely basis in the required manner. Confidentiality is the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner. Integrity is the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness. The relative priority and significance of availability, confidentiality and integrity vary according to the information system.

Threats to Information Systems

Technological development, technical problems, extreme environmental events, adverse physical plant conditions, human frailty, and inadequacies of social, political and economic institutions all present challenges to the smooth functioning of information systems. Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. They range from cataclysmic events to minor, daily inefficiencies. Down-times, for example, may be caused by one large break-down or frequent slow-ups or service degradations. The frequency and duration of disturbances, however minor, should be considered when planning for security. Large and small events may be equally disruptive to system functioning and use and equally debilitating to the organisation’s effective operation.

Technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They may be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads or other operational or quality problems. The difficulty may arise in an internal system component (system hardware and peripherals, such as a memory unit, a networked collection of computer systems or a distributed system; application and operating system software, such as a compiler or editor; LANs), an external system component (telecommunication circuits, satellites) or from the interaction of different parts of the system.

Technical problems may be caused by intentional attacks on the system. Viruses, often introduced into the system via infected software, parasites, trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort or destroy normal system functions.

The difficulty of providing security for networks and information is compounded in multiple-vendor environments. For example, a significant problem is the availability of access-control software, a commonly-used security measure, that is compatible with the entire system in a multiple-vendor environment. In order to facilitate development of effective security for information systems, standards bodies, governments, and vendors and users of information systems must agree on standards for security measures.

Physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms, and excessive heat and humidity. The information system may be housed in a building, in which, in addition to computers and communication lines located throughout the building, there may be dedicated computer rooms and data storage rooms. Connections for power supply and communication may lead to and from the building. Adverse physical plant conditions may arise from breach of physical security measures, power failures or surges, air conditioning malfunction, water leaks, static electricity and dust. An organisation may be affected by lapses either directly at its premises or indirectly at a vital point outside the organisation, such as power supply or telecommunication channels.

Human beings and the institutions they establish to reflect their values, whether social, economic or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users -- employees, consultants, customers, competitors or the general public -- and their various levels of awareness, training and interest compound the potential difficulties of providing security.

Lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users may not be aware of the potential for harm from system misuse. Poor security practices abound. Operators and users may not take even the most rudimentary security measures.

The choice of a password, a nearly universal user activity and usually a user’s first activity on a system, provides a striking example. Although passwords are employed to control access to most information systems, few users are instructed on the need for password security, on the manner in which to create a password or on penalties for misuse of the system. Without guidance, many users choose obvious passwords

that may be easily ascertained, such as family or pet names, joke words or words related to the task. After logging in to the system, untrained users may leave active terminals connected to network systems unattended, display passwords on the side of terminals, fail to create backup data files, share user identification codes and passwords, and leave open access-control doors into high security areas. These are threshold security problems that arise from entering a room, switching on a computer or terminal, possessing a password and logging in.

Errors and omissions may occur in gathering, creating, processing, storing, transmitting, and deleting data and information. Failure to back up critical files and software multiplies the negative effects of errors and omissions. If files have not been backed up, the organisation may incur significant expense in time and money in recreating them.

Intentional misuse of authorised system access and unauthorised system access ("hacking") for the purposes of mischief, vandalism, sabotage, fraud or theft are additional serious threats to system and organisational viability. Unauthorised copying of software (software piracy), for example, is widespread. Popular conception holds that the greater part of threats to information systems comes from external sources. On the contrary, persons who have been granted authorised access to the system may pose a larger threat to information systems. They may be honest, well-intentioned employees who, owing to fatigue, inadequate training or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorised access to tamper deliberately with the system for their own enrichment or to the detriment of the organisation.

Computer programs are an important element of information systems and a potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality and integrity of that system by overloading the system, changing the list of authorised users of certain parts of the system or altering data or information in the system. Violations of provisions of licensing agreements relating to the information system (e.g., software licensing agreements, database licensing agreements) may pose an additional security threat. Unauthorised alteration of the licensed program, for example, may trigger malfunctions as the modified software interacts with other parts of the system. Disclosure of proprietary information may damage an organisation’s competitive position.

Proper procedures must extend beyond the computer terminal and communication lines to the entire information arena. Improper handling of data and information storage media (whether paper, magnetic or other) and improper handling and disposal of discarded computer printouts may lead to security breaches. Computer printouts may contain proprietary or competitive information or clues regarding system access. Yet, many companies have no policy for their disposal. Once used for the organisation's purpose, they are considered worthless and discarded along with the day's used envelopes and pencil shavings. There may, however, be no expectation of privacy in trash, at least in trash that is outside the premises.

Insufficient use of systems may also lead to security problems, such as maintaining information availability or integrity in the event of shortages of qualified personnel, whether as a result of employees changing jobs, the introduction of new technologies requiring new skills, or work slowdowns, stoppages or strikes.

Social, political and economic institutions have not kept pace with technological development and growth in use of information systems. The price is uncertainty and lack of uniformity, which increase expense, cause delays and, if permitted to continue, might impede future growth. There is a glaring deficiency of codes of practice, standards, and legal guidance and apportionment of legal rights and obligations.

Harm Resulting From Security Failures

Security failures may result in direct and consequential losses. Direct losses are those to: the hardware, including processors, workstations, printers, disks and tapes and communication equipment; software, including systems and applications software for central and remote devices; documentation, including specifications, user manuals and operating procedures; personnel, including operators, users, and managerial, technical and support staff; and physical environment, including computer rooms, communications rooms, air conditioning and power supply equipment. Although direct losses may account for a small percentage of total losses arising from a security failure, nonetheless, the absolute investment in developing and operating the system will usually have been significant. The system requires protection in its own right as the container and channel for the data and information. The need to protect the system and the manner of doing so are inextricably linked to protecting the data and information that the system stores, processes and transmits in order both to preserve the availability, confidentiality and integrity of the data and information and to prevent alteration or damage of the container and channel through introduction of data and information, such as viruses, that may have a deleterious effect on operation and use of the system.

A consequential loss may occur when an information system fails to perform as intended. Consequential losses arising from security failures may include: loss of goods, other tangible assets, funds or intellectual property; loss of valuable information; loss of competitive advantage; reduction in cash flow; loss of orders or business; loss of production efficiency, effectiveness or safety; loss of customer or supplier goodwill; penalties from violation of statutory obligations; and public embarrassment and loss of business credibility. Consequential losses account for most of the losses arising from security lapses. In light of this fact, protection against consequential loss, which, above all, means protecting the data and information, must be a top priority.

Enhancing Security

The goals of confidentiality, integrity and availability must be balanced both against other organisational priorities, such as cost-efficiency, and against the negative consequences of security breaches. The cost must not exceed the benefit. Similarly, from the viewpoint of deterring those who would attempt to enter information systems to view, manipulate or obtain information, security controls should be sufficient to render the costs or the amount of time required greater than the possible value to be gained from the intrusion.

Adequate measures for security of information systems help to ensure the smooth functioning of information systems. In addition to the commercial and social benefits of information systems already mentioned, security of information systems may assist in the protection of personal data and privacy and of intellectual property in information systems. Similarly, protection of personal data and privacy and of intellectual property may serve to enhance the security of information systems.

The use of information systems to collect, store and cross-reference personal data has increased the need to protect such systems from unauthorised access and use. Methods to protect information systems include user verification or authentication, file access control, terminal controls and network monitoring. Such measures generally contribute both to the security of information systems and to the protection of personal data and privacy. It is possible that certain measures adopted for the security of information systems might be misused so as to violate the privacy of individuals. For example, an individual using the system might be monitored for a non-security-related purpose or information about the user made available through the user verification process might permit computerised linking of the user’s financial, employment, medical and other personal data. The principles of

the Guidelines (for example, the Proportionality Principle and the Ethics Principle) and those of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data give guidance in achieving compatible realisation of the goals of security of information systems and protection of personal data and privacy.

Information systems may include hardware, computer programs, databases, layout designs for semiconductor chips, data and information, elements of which may be protected by intellectual and industrial property laws. Intellectual property in information systems is intangible, may cross borders virtually imperceptibly, and may be vulnerable to theft by the effort of one finger in a matter of seconds without taking the original and without leaving a trace. Security of information systems may reinforce the protection of intellectual property by limiting unauthorised access to components of the system, such as software or competitive information.

Since contracts, transactions and disputes relating to information systems may involve parties, actions and evidence in many different jurisdictions, it may be useful to clarify existing rules or presumptions or to establish new ones with regard to the law applicable in matters relating to the security of information systems. Given that disputes related to the security of information systems may involve complex factual situations as well as parties, actions and evidence that may be situated in multiple jurisdictions, it may also be advisable to develop non-judicial means, including arbitration, for resolution of disputes.

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

Aims

This section of the Guidelines sets forth the purposes to be served by their formulation and adoption by governments and the private sector. The Guidelines are intended to assist the further development and use of information systems. In order to do so, it is viewed as necessary to raise awareness of risks to information systems and to provide reassurance as to the reliability of information systems and their provision and use. In recognition of the ubiquity of information systems, governments and the private sector are urged to co-operate to create an international framework for security of information systems. It is hoped that the Guidelines will contribute to increasing awareness of the importance of security of information systems and to dispelling reluctance to report security breaches, which might permit the compilation of more national and international statistics.

Scope

The Guidelines are intended to apply to all information systems, whether owned, operated or used by public or private entities or for public or private purposes. The information systems may be of a public or private nature and elements of them may be protected by intellectual property or industrial property laws or other laws (e.g., trade secrets, official secrets). The Guidelines are not intended to supersede or otherwise affect the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The objective of the Guidelines is full application at all levels. In particular, parties should strive to avoid the evolution of a dual approach, one for information systems related to national security and one for all other information systems. Notwithstanding these intentions, it is fully accepted that governments may find it necessary to depart from the Guidelines. This is the case in the areas of national security and maintenance of public order ("ordre public"). The fact that governments have the sovereign right to do what they must in these vital areas is recognised in the Recommendation of the Council Concerning Guidelines for the Security of Information Systems. However, it is expected that any departure from the Guidelines will relate more to the section on implementation than to the nine principles. The general idea is that exceptions to the Guidelines would be few and, since they relate to "sovereign" matters, would be of the highest order of importance. Furthermore, it was foreseen that appropriate information relating to departures from the Guidelines, whether involving a public or private information system, would generally be made known to the public and all interested parties.

Definitions

The definition of information systems includes: computer hardware; interconnected peripheral equipment; software, firmware and other means of expressing computer programs; algorithms and other specifications either embedded within or accessed by such computer programs; manuals and documentation on paper, magnetic, optical and other media; communication facilities, such as terminal/customer premises equipment and multiplexers, on the information system side of the network termination point of public telecommunication transport networks as well as equipment for private telecommunication networks not offered to the public generally; security control parameters; storage, processing, retrieval, transmission and communication data, such as check digits and packet switching codes, and procedures; data and information about parties accessing information systems; and user identification and verification measures (whether knowledge-based, token-based, biometric, behavioural or other). This definition may include elements that are proprietary or non-proprietary, public or private. This definition applies to elements whether or not they interact with the data being transmitted by the system or are necessary for the operation, use and maintenance of the other components of the system.

Confidentiality and integrity apply to data and information. The words data and information are repeated in the definition of availability, even though the term "information systems" includes them, in order to emphasise that availability also covers data and information. Confidentiality, integrity and availability may be important for reasons of competitive advantage, national security or in order to fulfil legal, regulatory or ethical obligations, such as fiduciary duties, protection of personal data and privacy or medical confidentiality. Examples of availability are up-time and response time of the information system.

Security Objective

43. The Principles of the Guidelines, which follow the Security Objective, express essential concepts to be considered in protecting information systems and providing for their security. The Principles are preceded by a simple declaration of the purpose and goals of security of information systems. Security of information systems is the protection of availability, confidentiality and integrity. In the absence of sufficient security, information systems and, more generally, information and communication technologies may not be used to their full potentials. Lack of security or lack of confidence in the security of information systems may act as a brake on information system development and use and on development and use of new information and communication technologies. One goal, therefore, is the protection of individuals and organisations

from harm resulting from failures of security. All individuals and organisations potentially rely on the proper functioning of information systems. Clear examples are the information systems in hospitals, air traffic control systems and nuclear power plants. Security, therefore, is directed at preserving the effectiveness of information systems. In addition to the goal of ensuring that the level of availability, confidentiality and integrity of information systems is not eroded, the security of information systems and the Guidelines are directed toward facilitating the development and use of information systems by individuals and for new and different purposes than those for which they are presently employed as well as toward facilitating the development and exploitation of information and communication technologies.

Principles

The Guidelines identify nine principles in connection with security of information systems. They are: the Accountability Principle; the Awareness Principle; the Ethics Principle; the Multidisciplinary Principle; the Proportionality Principle; the Integration Principle; the Timeliness Principle; the Reassessment Principle; and the Democracy Principle.

{Accountability Principle}

There should be an express and timely apportionment of responsibilities and accountability with respect to the security of information systems among owners, providers and users of information systems and others. The phrase "other parties concerned with the security of information systems" includes executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and internal and external information system auditors.

{Awareness Principle}

This principle is meant to assist those with a legitimate interest to learn of or be informed about security of an information system. It is not intended as an opening to gain access to the information system or specific security measures and should not be construed as tending to jeopardise security. The level of information sought pursuant to this principle should be able to be obtained without compromising security.

Owners and providers are included in the Awareness Principle for there may be circumstances in which they, too, may need to acquire information about the security of a system. For example, an owner of a network may enter into an agreement whereby another organisation would use the network to provide services for third parties. The owner may require, as part of the agreement, that certain levels of security be offered or available. In this circumstance, the owner may wish to be able to be informed of the security of the information system. Similarly, an organisation that contracts with a computer or network owner to provide services may desire assurances as to security and the ability independently to verify security. Users are also included in the Awareness Principle. For example, a customer choosing a bank may have a legitimate interest in being generally informed about the existence of security policies and programs of various banks. Depending upon customer demand, security might even come to be used as a marketing tool.

{ Ethics Principle}

Information systems pervade our societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information systems. This principle supports the development of social norms in these areas. Important aspects are the expression of these norms to all members of society and inculcation of these concepts from a very young age.

{Multidisciplinary Principle }

When devising and maintaining measures, practices and procedures for the security of information systems, it is important to review the full spectrum of security needs and available security options. In an organisation, for example, this would involve consultation with technical personnel, management, the legal department, users and others. All these groups will have different perspectives, requirements and resources that should be consulted and combined to produce an optimal level of security for the information system. Similarly, on a policy level, technical standards, codes of practice, legislation, public awareness, education and training for security of information systems may be mutually reinforcing.

From another aspect, this principle acknowledges that information systems may be used for very different purposes and that the security requirements may vary as a result. For example, the civil and military branches of government may have dissimilar needs for security as may different types of businesses or the commercial sector and private individuals.

{Proportionality Principle }

Every information system does not require maximum security. As it is important that systems not be insufficiently secure, so is it futile to provide security beyond the reasonable requirements of the system. Rather, there is a hierarchy of information systems and their security needs that differs for each organisation. For this reason, there is no one security solution.

In assessing security needs, the information should first be identified and a value assigned. Possible security measures, practices and procedures available to protect the various elements of the information system should be enumerated and the costs of implementing and maintaining each of the security options calculated. The level and type of security should then be weighed against the severity and probability of harm and its costs as well as the cost of the security measures. This analysis should be carried out for the information system in the context of all other relevant procedures and systems, including other information systems.

{Integration Principle}

Security of information systems is best considered when the system is being designed. Measures for security may be formulated and tested to avoid incompatibility. Overall costs of security may also be reduced. Security is required at all phases of the information cycle -- gathering, creating, processing, storing, transmitting and deleting. Security is only as good as the weakest link in the system.

{ Timeliness Principle}

In the environment of the interconnected information systems that span the globe, the importance of time and place are diminished. It is possible to gain access to information systems regardless of physical location. The Timeliness Principle acknowledges that, due to the interconnected and transborder nature of information systems and the potential for damage to systems to occur rapidly, parties may need to act together swiftly to meet challenges to the security of information systems. Depending upon the security breach, the relevant parties may be members of the public and private sectors and may be located in different countries or jurisdictions. This principle recognises the need for the public and private sectors to establish mechanisms and procedures for rapid and effective co-operation in response to serious security breaches.

{Reassessment Principle }

This principle recognises that information systems are dynamic. System technology and users, the data and information in the system and, accordingly, the security requirements of the system are ever-changing. The information systems, their value, and the severity, probability and extent of potential harm should, therefore, undergo periodic reassessment. Follow-up is as important as implementation, especially in light of new technological developments, whether those adopted by the system owner or those available for use by others.

{Democracy Principle}

The security interests of owners, developers, operators and users of information systems must be weighed against the legitimate interests in the use and flow of information with the aim of striking a balance in accordance with the principles of a democratic society. Those unfamiliar with security of information systems may presuppose that security of information systems may lead only to restrictions to access to and movement of data and information. On the contrary, security may enhance access and flow of data and information by providing more accurate, reliable, and available systems. For example, harmonization of technical security standards will help to prevent data and information islands and other barriers to data and information flows.•••

Implementation

National governments should strive to ensure that territorial subdivisions in their countries are aware of the Guidelines and their implications for areas within the competence of the subdivisions. They should communicate at political level to all territorial subdivisions the text of the Guidelines, undertake every effort to urge their implementation, and consult as to difficulties that may arise.

Self-regulation may take the form of codes of conduct or practice developed and adopted by individual organisations, industry or professional associations or public sector agencies.

{Policy Development}

Worldwide harmonization of standards

There is a need for creation of appropriate technical security standards (including product and system evaluation criteria) with the widest possible geographic range of applicability. Their development should be the product of collaboration between, among others, governments, standards bodies, and vendors and users of information systems.

While seeking harmonized standards, it should be recalled that, as to individual situations, there can be no one security solution. Security needs vary considerably from sector to sector, company to company, department to department, and, as to given information systems, over time. Lack of an informed and balanced understanding of users' needs may create a significant risk of "off-target" technology standardisation. A productive first step is recognition of the inherent diversity and heterogeneity of users' needs for information system safeguards.

Promotion of expertise and best practice

Governments, public sector agencies, industry and professional associations and organisations should work together to promote expertise and to develop and promote awareness of concepts of "best practice" in the field of security of information systems. This may include notions of risk analysis, risk management, insurance, or audits. The particular program adopted may vary from organisation to organisation and from sector to sector. The security requirements of the banking sector, for example, may differ from those of other sectors. •

Contract formation and validity

The goals of parties to an electronic transaction are not very different from those in a paper transaction. Generally, the participants in an information transfer, whether electronic or non-electronic, want to know that the information came from the person who purports to have sent it, that it is received only by persons intended to receive it, and that it arrived in the intended form, unaltered and unmanipulated. While the goals of parties to electronic and non-electronic transactions may be basically the same, the manner of achieving these aims are not. They differ as a function of the means of creation, use, transmission, storage, and access to electronic and non-electronic information. The manners in which the two types of information are protected perforce differ as well.

The challenge is to bring to electronic dealings the same level of confidence that presently exists for paper transactions. This may be accomplished in several ways. First, existing rules may be applicable to electronic situations. As necessary, existing rules may be modified and new ones developed. Technological means may also be employed. Further study and refinement of commercial laws involving electronic transactions might be useful, including rules relating to the validity of electronic signatures, the formation and validity of contracts created and executed in information systems, and enforcement of and liability for such contracts.

Allocation of risks and liability

There seems to be a dearth of rules relating to allocation of risks and liability for damage arising from security lapses. The relevant parties may include vendors, distributors, telecommunication operators, service providers and users. Several systems may be involved in an information transfer, often including systems outside the ownership or control of the information processor or transmitter. The rights and duties of the parties involved may be unclear in cases of mistakes, omissions, failures of the various systems or other mishaps.

The need for such rules exists and is illustrated when funds that are electronically transferred between two financial institutions are lost or stolen. Such transfers may involve vast amounts of money, are common financial practice, and are made almost instantaneously and across international boundaries. Where existing rules are not sufficient, further development and refinement on the national and international levels on the manner in which to assign liability in cases of fraudulent or negligent wire transfers is supported.

Sanctions

Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime.* National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems.

_____

* See, e.g.:

Organisation for Economic Co-operation and Development (1986), {Computer-Related Crime: Analysis of Legal } {Policy}, ICCP Series No. 10;
Council of Europe (1989), Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems;

At the same time, it is recognised that many factors may aggravate or mitigate the seriousness of the conduct: the specific intent of the actor, the type of data affected (e.g., national security or medical data), the extent of the harm, and the extent to which the actor exceeded authorisation. For minor violations, the use of administrative sanctions, such as the imposition of non-penal fines by an administrative agency, is considered by some nations (especially in the area of data protection) to be sufficient. Other types of sanctions may include, for example, disciplinary measures against civil servants or civil sanctions.

The development of legislation in OECD Member countries has already led, particularly under the influence of international organisations, including the OECD, to a certain degree of harmonization. In order to further international co-operation in penal matters (including in the areas of mutual assistance, extradition and other international co-operation described below), this harmonization process should be supported and taken into account by countries when reviewing their legislation.

Jurisdictional competence

In addition to the jurisdictional competence of courts in matters relating to the security of information systems, some countries may wish to grant certain administrative agencies rights to impose administrative sanctions.

The transborder character of data flow on the one hand and the mobility of offenders on the other hand may create problems in prosecuting computer criminals. Ideally, there should be harmonized rules on extraterritorial jurisdiction. However, pending the development of such rules, individual countries should review the suitability of their domestic jurisdictional rules to deal with transborder offences. In countries where the doctrine of ubiquity (a crime is committed where one of its elements takes place) is not acknowledged, difficulties arise as to the application of national computer crime laws. In such countries, it may be necessary to introduce special jurisdictional rules, as, for instance, was done in the United Kingdom, where the Computer Misuse Act 1990 claims jurisdiction when the hacker or computer is in the United Kingdom or where the interference makes use of a computer in the United Kingdom.

_____

.../...

United Nations (1990), Statement on Computer-related Crime, Report of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August-7 September; and

International Chamber of Commerce (1988), {Computer Related } {Crime and Criminal Law: An International Business } {View}, Position Paper No. 11, June.

If a national of a state commits a computer-related crime in another state, problems may also arise when the crime is detected and the perpetrator is in the home country. Many countries do not extradite nationals. In such situations, an extension of the existing rules of extraterritorial jurisdiction (or the possibility of transfer of proceedings (see the following paragraph)) should be considered with a view to creating the necessary prerequisites for a successful prosecution in at least one state.

Mutual assistance and extradition

Mutual assistance agreements, extradition laws, recognition and reciprocity provisions, transfer of proceedings and other international co-operation in matters relating to the security of information systems may facilitate assistance to other countries in their investigations.

Evidence

Improved security of information systems, by enhancing the accuracy, completeness and availability of data and information in the information system and, accordingly, by increasing the ability to rely on data and information in the system, may assist the introduction and use of such evidence in legal and administrative proceedings. Similarly, in legal systems with special formal requirements regarding evidence, clear rules of evidence in both penal and civil legal and administrative proceedings may make information systems more secure by providing more predictability in actions involving failures or breaches of security and by the potentially deterrent effect of such actions.

At present, electronic records may present problems for existing laws of evidence. For European continental countries, which have civil law systems, the admissibility of evidence in court is based upon the principle of free introduction and free evaluation of evidence. This is also the situation in Japan with respect to non-penal matters. In theory, under such legal systems, a court may admit any material as evidence, including computer records, but it must then decide the value such material will be afforded as evidence.

In common law countries, however, the admissibility of evidence is subject to objection and governed by complex rules. Computer records, like any other documents, may present two issues. The first is authentication: Are the documents accurate and genuine? Are the printouts from the computer admissible either as "originals" or "copies" of the data in the system? In the United States, for example, the federal rules expressly allow authentication and admission of computer records. The second issue that common law systems must address with respect to any document is whether it contains hearsay. This pertains not to the form of the document (whether electronic data or handwritten) but to its content. Generally, it is possible to testify only

about matters of which one has direct knowledge and not about something learned from secondary sources. This rule applies to documents as well as to individuals and, while the hearsay rule has many exceptions (the business records rule, for example), this issue must be recognised and anticipated.

{ Education and Training}

An overarching task is the increase of awareness at every level of society, in governments and the private sector and among individuals, of the necessity for and the goals of security of information systems and good security practices. Promotion of awareness should also include awareness of the risks to information systems and of safeguards available to meet those risks. It is important to develop social consensus about proper use of information systems.

In building awareness, it is essential to have the co-operation of users of information systems and the commitment of management, especially senior management, to providing for security of information systems.

Education and training should be included in school curricula and should be provided for users, executive management, programmers, maintenance providers, information system managers (software managers, operations managers, and network managers), software development managers, managers charged with security of information systems, and auditors of information systems and of security of information systems, both internal and independent auditors. Trained, professionally qualified auditors should inspect and evaluate an information system. Information system auditors should possess knowledge of planning, development and operation of information systems and of general auditing and should have actual experience in performing information system audits. It is equally important that law enforcement authorities, including police and investigators, and attorneys and judges receive adequate education and training.

{ Enforcement and Redress}

There should be provided accessible and adequate means for exercise and enforcement of rights related to the security of information systems and for recourse and redress of violations of such rights. This includes access to courts and provision of means for adequate investigative powers. Security breaches include failures and violations of security of information systems. There is a need for better cross-education, communication, co-operation and sharing of information among law enforcement agencies, communications operators and service providers, and banks at national and international levels. Law enforcement authorities should co-operate to facilitate investigations in other countries.

{Exchange of Information}

Governments, the public sector and the private sector should exchange information and establish procedures to facilitate the exchange of information relating to the Guidelines and their implementation. As part of their efforts, they should publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems. It is desirable that national governments make known to the OECD, other international bodies and other governments their activities and those of their territorial subdivisions relating to the security of information systems, the Guidelines and their implementation.•

{Co-operation}

Governments, the public sector and the private sector should develop measures, practices and procedures that are simple and compatible with those of other parties that comply with the Guidelines, taking into consideration in their development the measures, practices and procedures developed by others, so as to avoid, where possible, conflicts or obstacles. All laws adopted on regional, national or provincial levels should be harmonized to meet the challenges of a worldwide technology.

END-OF-TEXT