Guidelines Necessary

Guidelines Necessary

Michael D Kirby
President, Court of Appeal,
NSW Supreme Court, Sydney

In the past decade it became clear that a number of interrelated problems, presented by information technology, required intergovernmental attention. In particular, three issues continued to cause concern amongst major users of information technology. They were the reports of the steadily increasing incidence of computer-related crime, a new phenomenon of computer "hacking" and the introduction of highly damaging computer viruses.

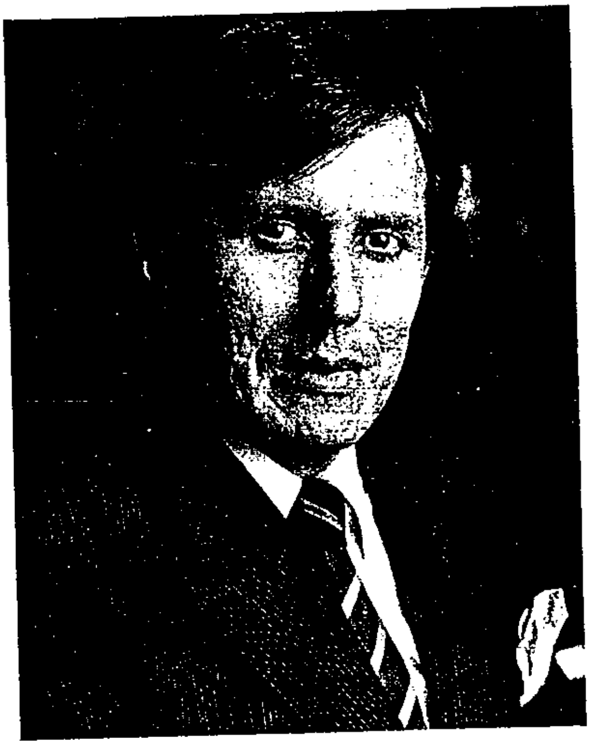
The OECD itself maintained, under one of its committees, a continuing scrutiny of the issue of computer crime. The economic significance of computer crime for societies increasingly dependent upon the reliability and accuracy of computer records, was obvious. Other international bodies also showed a lively interest in the topic. In 1989 the Committee of Ministers of the Council of Europe adopted a recommendation on computer-related crime. They urged moves to harmonization of the law and practice of European countries on computer crime and for improved international legal cooperation to deal with such crime wherever it had a transborder characteristic.

Specifically, the report of the Council of Europe put forward a minimum list of subjects that should be covered by computer crime legislation (computer fraud; computer forgery; damage to computer data or programs; computer sabotage; unauthorized access; unauthorized interception; unauthorized reproduction of a protected program and unauthorized reproduction of topography). It also described an "optional list of offenses (alteration of computer data or programs; computer espionage; unauthorized use of a computer and unauthorized use of a protected computer program).(1)

OECD Guidelines In *TDR*

The complete text of the OECD Guidelines for the Security of Information Systems, adopted on November 26, 1992, were published in *TDR*, January/February 1993, pp 30-32.

On a wider stage the United Nations became involved in the issue of computer crime. In the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Cuba in September 1990, a report was adopted affirming the need for the development of "appropriate international action" by member states to "more effectively combat computer abuses that deserve the application of criminal sanctions."(2)



Kirby

The problem of computer "hacking" and the introduction of viruses attracted widespread attention when it was shown, in the United States, that an offender, Robert T Morris Jr., had introduced a "worm" into information systems with consequences involving financial losses to those affected estimated by the prosecution to amount to US$ 97 million. Morris claimed an intention merely to show the vulnerability of the systems to intrusion. He was prosecuted and convicted under the Computer Fraud and Abuse Act (US).

His conduct was illustrative of others whose viruses attracted such exotic names as the "Internet worm," the "Christmas tree virus," the "AIDS Trojan horse" and the "Italian bouncing ball virus." The AIDS Trojan horse involved an attempted extortion. Its perpetrator was arrested in Cleveland (US) on a warrant issued in London, from where most of the offending diskettes containing the virus were posted worldwide.

As a consequence of these and similar acts, the Computer, Science and Telecommunications Board of the United States established a committee in 1990 to develop a national strategy on computer viruses. Its first recommendation was the promulgation of a comprehensive statement of generally accepted systems security principles.

There have been other national and sub-national reports drawing attention to specific problems of computer crime, the vulnerability to intrusion, manipulation and distortion of many automated information systems. In Australia the October 1992 *Report on Unauthorized Release of Government Information*(3) of the Independent Commission Against Corruption (NSW) demonstrated a "shockingly widespread illicit trade in information held in the public sector." The trade operated between government officials, commercial firms and private inquiry agents. Information from federal and state government sources and the private sector was sold for private gain.

It is against the background of these developments that international initiatives, including those of the OECD, must be understood.

OECD expert group

In February 1990 in Toronto, Canada an international meeting was organized supported by a number of major international banks. International financial transactions are, potentially, especially vulnerable to intrusion, manipulation and crime affecting their transborder data flows. As a result of the Toronto meeting a statement was issued by the participants urging renewed attention by the OECD to the issues of policy presented by the dangers to the security of information systems.(4)

A number of the participants in the Toronto meeting (including the writer) had played a part in the OECD Expert Group on Privacy. Many were to participate in its forthcoming work on data security.(5) The result of the Toronto statement was a further impetus to the OECD to establish a new group on Security of Information Systems. The OECD had maintained a steady interest in security systems. In October 1988 one of its committees approved preparation of a study on the subject of security of information systems. The result was a report on *Information Network Security* in 1989.

It was the review of this document which led the OECD Committee for Information, Computer and Communication Policy (ICCP) to convene the Expert Group which produced the Security Guidelines. The writer was again elected chairman. Similar procedures were followed as in the earlier committee which prepared the Guidelines on Protection of Privacy and Transborder Flows of Personal Data. In a series of six meetings, the last in September 1992, Guidelines were produced for submission to the ICCP Committee and to the OECD Council for approval in November 1992.

There was one feature of the second Expert Group on Data Security which distinguished it from the Privacy Group. A substantial contingent of experts from the private sector and from the trade unions participated in the discussions with the representatives and experts from the OECD member countries. As well, particular care was taken by the Secretariat officers in charge of the project (Hans-Peter Gassmann and Deborah Hurley) to consult widely with interested groups and to ensure that their comments on the Guidelines, as they were developed, were taken into account in the deliberations of the Group. Perhaps as a result of this the Guidelines were quickly adopted both by the ICCP and by the OECD Council. The latter approved the Guidelines on November 26, 1992. They were recommended by the OECD Council for action by member countries.

Guidelines' main provisions

In a press statement issued following the adoption of the Guidelines it was pointed out that information systems play an increasingly significant and pervasive role in national economies, international trade, government and business operations, health care, energy, transport, communications and education. The need for security for such systems required the protection of their availability, integrity and confidentiality. These three features of data security are well established.(6) According to the OECD statement:

"While growing use of information systems has generated many benefits, it has also shown up a widening gap between the need to protect systems and the degree of protection currently in place. Society has become very dependent upon technologies that are not yet sufficiently dependable. All individuals and organizations have a need for proper information system operation (e.g., in hospitals, air traffic control and nuclear power plants). Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise the systems and their underlying technologies may not be used to their full potential, and further growth and innovation may be inhibited."(7)

The Security Guidelines now adopted by the OECD Council follow, in part, the pattern of the earlier Privacy Guidelines. They are accompanied by a recommendation of the Council of the OECD which recites the increasing use and value of information systems; the international nature and worldwide proliferation which has occurred; the growing interdependence of national and internatonal economies as well as social, cultural and political life; the risks arising from inadequate safeguards; and the need to raise awareness of those risks and to respond appropriately to violations of security.

The recommendations of the OECD Council recognize that the Guidelines do not affect the sovereign rights of national governments on matters such as national security determined in accordance with national law. There is also a recognition (relevant to countries such as Australia, Canada, the United

States and Germany) that, in federal countries observance of the Guidelines may be affected by the local constitutional division of powers.

This said, the recommendations now adopted by the OECD Council recommend that member countries establish measures, practices and procedures to reflect the principles contained in the Guidelines; that they consult, coordinate and cooperate in their implementation; that they agree as expeditiously as possible on specific initiatives; and that they disseminate the principles of the Guidelines widely and review them every five years with a view to improving international cooperation.

It is now up to member countries of the OECD, and others, to consider the Guidelines and to commence the long process of bringing laws and practices into conformity, just as was earlier done following the adoption of the Privacy Guidelines.

Other data law initiatives

It is worth noting that the OECD initiative on security of information systems has been running in parallel with other initiatives taken by other international bodies. One group which has been interested in issues of data security is the meeting of Data Protection Commissioners. Chaired by the Australian Privacy Commissioner (Kevin O'Connor) that group held its first meeting in Australia in November 1992.

Even more immediately influential is the current work of the Commission of the European Community. It has proposed a Council Directive on Data Protection.(8) In late 1990 such a directive was put forward in draft form. Further work on data security protection is also proceeding in the Council of Europe. The early completion by the OECD of its project seems likely to ensure that the OECD Guidelines are influential in shaping national and international laws and policies on this topic.

Footnotes

[1] Council of Europe, European Committee on Crime Problems, *Computer-related Crime*, Strasbourg, 1990, p 14.

[2] United Nations Eighth Congress on the Prevention of Computer Crime and the Treatment of Offenders, *Report on the Prevention of Crime and Treatment of Offenders*, p 147 (A/Conf.144/28).

[3] See New South Wales (Australia), ICAC, *Report on Unauthorized Release of Government Information*, Sydney, 1992. See also A Roden, "Computer Crime and the Law" (1991) 15 *Crim LJ*, p 397. See also S Davies, *Big Brother: Australia's Growing Web of Surveillance*, Simon and Schuster, Australia, Sydney, 1992, p 100, and I Temby, "Australia Exposes Illegal Data Sales" (1993) 16, *Transnational Data Report*, p 26.

[4] M D Kirby, "Toronto Statement on the International Legal Vulnerability of Financial Information," 11 *Computer/Law Journal* (1991), p 75. See also L J Hoffman (ed) *Rogue Programs: Viruses, Worms and Trojan Horses*, Van Nostrand Reinhold, New York, 1990 and United States National Research Council, *Computers at Risk*, National Academy Press, 1991.

[5] Including R Buxton QC (UK), M Horibe (Japan), W List (UK), Y Mine (Japan), D Piragoff (Canada) and B de Schutter (Belgium).

[6] But note that some experts suggest two further criteria of information security, *viz* "utility" and "availability." The OECD Expert Group did not accept these notions as central to the security idea.

[7] OECD press statement, "OECD Adopts Guidelines for the Security of Information Systems," November 27, 1992 (92/86).

[8] European Communities, *Proposal by the Commission for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data* (COM[90]314), Brussels, September 1990.

Michael D Kirby, President, Court of Appeal, Supreme Court of New South Wales, GPO Box 3, Sydney, NSW 2001, Australia.

Justice Kirby served as chairman of the OECD Working Group on Security of Information Systems, which drafted the OECD Guidelines.