Guidelines for the Security of Information Systems

Extracted below is a brief outline of the recently drafted recommendations of the OECD Committee for Information, Computer and Communications Policy. These recommendations are for guidelines for the security of information systems.

Extracted below is a brief outline of the recently drafted recommendations of the OECD Committee for Information, Computer and Communications Policy. These recommendations are for guidelines for the security of information systems.

In March 1990, the Committee for Information, Computer and Communications Policy (ICCP) of the OECD approved the creation of a Group of Experts to draft Guidelines for the Security of Information Systems. In September 1992, the Group approved the submission of the Guidelines to the Committee together with recommendations concerning the Guidelines and an explanatory memorandum.

The Guidelines are intended to provide a foundation from which countries and the private sector can construct a framework for security of information systems; the framework to include laws, codes of conduct, technical measures, management and user practices, and public education and awareness activities.

The Group recognised the significance of computer and communications technologies, economically, socially and politically, and that information systems benefit governments, international organisations, private enterprise and individuals. Because of the fact that such systems *are* so beneficial, and, in some cases, critical, dependence on information systems is growing and there is a mounting need for confidence that they will continue to be available and to operate in the expected manner.

However, according to the Group, that dependence is upon technologies that are not yet sufficiently dependable. There are risks of loss from malfunctions of hardware and software, unauthorised access, use, misappropriation, modification or destruction, which may be caused accidentally (such as in the case of extreme environmental events, and that of human users with various levels of awareness and training), or result from purposeful activity (such as hackers and viruses). Such failures may result in direct financial loss, such as loss of orders or payments, or more indirect, less quantifiable losses, such as disclosure of personal information.

The Group recognises that users must have confidence that information systems will operate as intended, or the systems will not be exploited to the extent that further growth and innovation may be inhibited.

The Group sees security of information systems as the protection of availability, confidentiality and integrity. Such goals must, however, be balanced against both other organisational priorities, such as cost-efficiency, and against the negative consequences of security breaches.

The Guidelines identify nine principles in connection with security of information systems:

- the Accountability Principle, which relates to an express apportionment of responsibilities and accountability among owners, providers and users of information systems;
- the Awareness Principle refers to those with a legitimate interest for learning or being informed about security of systems;
- the Ethics Principle, which supports the development of social norms in relation to the use and security of information systems;
- the Multidisciplinary Principle acknowledges that information systems may be used for very different purposes and that the security requirements may vary as a result;
- the Proportionality Principle recognises that all systems will not require the same level of security;
- the Integration Principle refers to the desirability of security being considered when the system is being designed;
- the Timeliness Principle acknowledges that, due to the transborder nature of information systems, parties may need to act together swiftly to meet challenges upon security;
- the Reassessment Principle recognises that information systems are dynamic, and that, therefore, their security systems should undergo periodic reassessment; and
- the Democracy Principle refers to the weighing up of the security interests of owners, developers and users, against the flow of information.

The Group sees the methods of implementation of the Guidelines in developing security for information systems as including:

- worldwide harmonisation of technical security standards;
- promotion of expertise and best practice;
- bringing to electronic dealings the same level of confidence that presently exists for paper transactions;
- the creation of rules relating to allocation of risks and liability;
- ensuring sanctions for misuse are adequate;
- ensuring jurisdictional competence of courts and administrative agencies;
- co-operation between countries including extradition laws and transfer of proceedings;
- the development of clear rules of evidence in both penal and civil proceedings;
- education and training to increase the awareness of the necessity for security;
- provision of accessible and adequate means for enforcement of rights related to security; and
- the exchange of information and co-operation relating to the Guidelines and their implementation between governments, the public sector and the private sector.

For a full copy of this report please contact The Editors.

In conjunction with

THE 1993 BIENNIAL COMPUTER LAW CONFERENCE - DOING BUSINESS IN THE PACIFIC RIM

The New South Wales Society for Computers and the Law invite The Faculty and Delegates of the Conference and Members of the Society to a Cocktail Party to be held on the final evening of the Conference.

Date: Friday 26 February 1993
Time: 5.15pm to 7.00pm
Venue: Level 34, AMP Centre, 50 Bridge Street, Sydney

For more information please contact:

Connie Carnabuci
Mallesons Stephen Jaques
Ph: (02) 250 3000