International Working Group
on Data Protection
in Telecommunications

675.29.7 19 November 2004

Working Paper
on
Cyber Security Curricula Integrating National, Cultural and Jurisdictional (Including Privacy) Imperatives

- adopted at the 36th meeting on 18-19 November 2004 in Berlin -

Information Systems Security

In the early stages of computerization, information systems security was predominantly concerned with modest stand-alone systems in closed networks and was accordingly limited in scope to the adoption of relatively simple rules of physical, computer and logical security.

Subsequently, the proliferation of more and more powerful personal computers, the popularization of new information and communication technologies, the widespread use of the Internet, and the increasing dependence of human activities on the proper functioning of information systems have made the situation more complex.

Today, information systems security can no longer just be limited to palliative countermeasures vis-à-vis technological security threats but needs to involve fundamental changes to behavior patterns by all the participants in order to address the pervasive threats posed by cyber security to human values and human rights.

This new global and systemic approach of the information security has been underlined and put forward by the OECD whose publication *'Guidelines for the security of information systems and networks'* includes a recognition of the need to develop a real 'culture of security'[1].

Information systems security vs. personal data protection

Today, to attain their respective objectives, all the organizations, whether governmental or private, are required to collect, process and retain an increasing volume of data including more personal data within their information systems.

Privacy is a fundamental human right and the valid protection of personal data cannot be achieved without adequate security. This has already been recognized in 1980 by the '*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*'[2]. Whilst security is mandatory to achieve privacy, personal data benefit from specific statutory protection compared with other data and their security requires often a totally different approach. The fundamental data protection princi-

[1] Recommendation of the OECD Council at its 1037th Session on 25 July 2002 : '*OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security'.*

[2] Recommendation by the Council of the OECD adopted on 23rd September, 1980 : *'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' – Security safeguard principles.*

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

ples such as the right of oblivion (right to erasure of obsolete data), the right of access, the limitation of collection and use and the proportionality principle, are regrettably not basic principles to which security professionals necessarily subscribe.

Information Security Professionals

Nowadays information systems security has to deal not just with the technological risks of the various computer platforms, networks, protocol or others components of the information systems but has also to take into account other risks such as those connected with the organization of the company, with its work method, those linked to its personnel or those concerned with the legal constraints in force such as data protection or intellectual property.

This multidisciplinary perception of the risks is not the rule in the world of information systems security professionals. Too often, information systems security is still considered just as a computer or technical expert business and then merely limited to prophylactic technical measures, with as a consequence, complex security systems based on a proliferation of technical controls of dubious relevance that may compromise personal privacy.

Even if the need for highly skilled security professionals is more widely recognized, few concrete structural initiatives are taken to meet the existing expectations in this domain. Often the concept of the Information Systems Security Adviser is neither introduced, defined nor framed by any legal text and access to the 'profession' is left to a certification process organized by private international companies.

Recommendations

Vis-à-vis this situation, the Working Group, quite aware of the primordial roles that information systems security and data protection play in the proper functioning of any organization, recommends that :

- The concept of Information Systems Security Adviser, corresponding to the CISO concept (Corporate Information Security Officer) described in several international standards[3] and publications[4] and which includes all the necessary data protection aspects, should be supported.
- In view of the responsibilities involved when carrying out such a function there is undoubtedly a need for greater professionalism. Very often such functions require university degrees. Accordingly, an academic or professional qualification should be dedicated to Information Systems Security Advisers that would provide an education according to their national legal and cultural traditions and that would be as neutral and independent as possible of any commercial interests. This qualification should certify all the necessary technical security skills, the relevant management skills, the knowledge of how security can best be managed, knowledge of fundamental data protection concepts and finally all relevant legal skills[5] that would enable security advisers to fulfill their role correctly within an organization.

[3] ISO 13335 : *'Information technology – Security techniques - Management of information and communications technology security'* and ISO 13569 : *'Banking and related financial services - Information security guidelines'* .

[4] Different documents published by different national organizations such as NIST (*National Institute of Standards and Technology*) – US, CSE (*Communications Security Establishment*) - Canada and DCSSI *(Direction Centrale de la Sécurité des Systèmes d'Information)* – France.

[5] ISO/IEC 17799 'Information technology – Code of practice for information security management' expressly refers to national laws which have to be followed even if the standard is complied with.