Distr.
GENERAL

CES/SEM.47/11 (Summary)
9 January 2002

Original: ENGLISH

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE | **COMMISSION OF THE EUROPEAN COMMUNITIES**

CONFERENCE OF EUROPEAN STATISTICIANS | **EUROSTAT**

Joint UNECE/Eurostat Seminar on Integrated Statistical Information Systems and Related Matters (ISIS 2002)
(17-19 April 2002, Geneva, Switzerland)

Topic II: Secure communications and data confidentiality

THE PRACTICE OF SAFE COMPUTING

Invited paper

Prepared and submitted by Eduardo Gelbstein[1]

Summary

1. Information Security has become a highly visible subject as a result of the widespread circulation of computer viruses and events such as the misuse of credit card information. However, the need to protect information is as old as the history of writing, i.e. some 5,000 years old.

2. This paper consists of two parts. Part I presents an overview of "Players" and "Offences". The *players* are the many parties active in the field of information security, ranging on the side of the Bad Guys from script kiddies (usually young computer enthusiasts who acquire the tools used by more knowledgable hackers) to industrial spies, organized crime and the intelligence services of "other" countries, and on the side of the Good Guys, security practitioners, auditors, etc. The *offences* are those acts which impact on the availability, confidentiality and integrity of information held in digital form. Such offences go well beyond viruses and include fraud and sabotage, the theft of proprietary information and software, the use of malicious code, denial of service attacks and other, all of which are described in some detail in the paper.

3. Part 2 is a practical guide to the *practice of safe computing*. Whilst in a corporate environment, there are (or should be) policies, guidelines, tools and technologies dedicated to ensure an adequate level of information security, there is a growing trend towards the use of home, mobile and wireless computing outside the corporate security perimeter.

4. The practice of safe computing requires several components to come together. These are:

- Tools, e.g. virus detection software and personal firewalls;
- Systematic use of processes, e.g. regular backups and updating virus definitions;
- Applied "common sense", e.g. non-disclosure, dealing with suspect e-mail and awareness of what offences are possible.

This part of the paper discusses all three in sufficient detail for a reader to put these things into practice.

[1] Independent consultant on the management of information systems and technologies (ed.gelbstein@wanadoo.fr).