

# APEC and OECD Strategies for Security of Information Systems & Networks Workshop

Keith Besgrove

Vice Chair, Working Party on Information  
Security and Privacy, OECD

## The Commons

- ▶ The Commons were tracts of community owned land in England.
- ▶ The Boundaries were known.
- ▶ Security was based on mutual trust.
- ▶ But, damage was caused by overuse.



## Other Types of Commons

- ▶ The 'high seas' have been considered a commons to support international trade routes and fishing.
- ▶ To protect it - Governments have developed International Conventions on the Law of the Sea.
- ▶ Air space is another commons - heavily regulated to facilitate air travel.



## The Internet is the New Commons

- ▶ Like the English Commons, the High Seas, and international airspace, no one owns the internet.
- ▶ Boundaries on the internet are virtual.
- ▶ The internet is now a place (or space) of commerce of growing value.
- ▶ However, like the commons before it the internet has attracted its share of abusers.
- ▶ Cyber-crime and cyber-terrorism are very real threats.

## OECD Principles

The OECD Culture of Security is based on nine complementary Principles,

- ▶ Awareness
- ▶ Responsibility
- ▶ Response
- ▶ Ethics
- ▶ Democracy
- ▶ Risk Assessment
- ▶ Security Design and Implementation
- ▶ Security Management, and
- ▶ Reassessment



## Objectives of the Security Guidelines

- ▶ Guide the development of consistent national policies to help address security threats and vulnerabilities in a global interconnected society, while preserving important societal values such as privacy and individual freedom.
- ▶ Develop a “Culture of Security” across society, so that security become an integral part of the normal way individuals, businesses, and governments use ICT and conduct online activities.

## The current state in the OECD

- ▶ National multidisciplinary and multi-stakeholder approach
- ▶ High-level governance structure
- ▶ National information policy framework
- ▶ Legal frameworks for combating cybercrime
- ▶ Computer Emergency Response Teams (CERTs) - Computer Security Incident Response Teams (CSIRTs).

## Main areas for further progress

- ▶ Research and development
- ▶ Measuring effectiveness of national policies
- ▶ Initiatives to address the needs of small and medium enterprises (SMEs).
- ▶ The role of identity management in relation to security of information systems and networks
- ▶ Identifying potential new threats and exploring ways to cope with them

## APEC/OECD Workshop Agenda

- ▶ Spyware – defining spyware, what it does, why it is a threat, and how it relates to malware.
- ▶ Reaching out to Small and Medium Enterprises and Individuals.
- ▶ Promoting Effective Global Incident Response.
- ▶ Emerging Security Threats and Technologies being developed to Address them.
- ▶ Comparing Legislative and Policy Approaches to Identity Management and to Security of Information Systems and Networks.



Exchanges such as this workshop are needed to lead us to the global collaboration needed to protect the internet as an important resource.

Thank You