The expanding deployment and use of information systems and networks by SME’s and individuals increases the necessity for focusing on securing their systems. What efforts by government are most successful in reaching this segment of users? How is the industry that supplies the hardware, software and services for SME’s and individuals responding to their needs?
Presentations

- **Introduction to Security and SME’s**
  - Ms. Jan Gessin, Asia Oceania Electronic Marketplace Association (AOEMA)

- **Business Perspective on Security Fatigue**
  - SIFT Australia, Nick Ellsmore

- **Best Practice of ISMS Implementation in Environments with Limited Resources**
  - Ms. Li-Hsuan Liang, NII Enterprise Promotion Association, Chinese Taipei

- **National Cybersecurity Alliance: a US initiative geared toward educating SME’s and home users on cybersecurity**
  - Sallie McDonald Special Assistant to the Assistant Secretary for Infrastructure Protection, DHS (USA) – on behalf of the National CyberSecurity Alliance

- **Addressing Information Security Needs of Users – Practical experience at the OECD**
  - Peter Lübkert, Head of Division, Information Technology and Network Services, OECD

---

Ms. Jan Gessin
jan.gessin@aoema.org
Asia Oceania Electronic Marketplace Association (AOEMA)

**Introduction to Security and SME’s**

- **Key Points** – SME’s too small – “it will never happen to me”
  - Lack of knowledge of the risk of assets loss
  - Low awareness - unaware that their computers contains assets that are valuable for their business
Mr. Nick Ellsmore
nick.ellsmore@sift.com.au
SIFT Pty Ltd, Australia

Business Perspective on Security Fatigue

Key Points – Define Security Fatigue –
Defined as desensitized as to security risks although risks are still there.

familiarity - example STD’s going up, Car deaths rising from 9th to 3rd in the world

Leadership ion SME’s important –
Founders/owners to obey good practice
that they preach to employees

Ms. Li-Hsuan Liang -
lliang@nii.org.tw
National Information Infrastructure
Enterprise Promotion Association

Best Practice of ISMS Implementation in Environments with Limited Resources

Key Points - Chinese Taipei is proposing a Government mandated security program including training and certification inc training for trainers for SME’s

Using BS7799/CNS17800 standards as a baseline but redefined for SME’s

Taking security out of the high risk end user environment – Schools to the local server network
Sallie McDonald
sallie.mcdonald@dhs.gov
Department of Homeland Security (DHS), United States

National Cybersecurity Alliance: a US initiative geared toward educating SME’s and home users on cybersecurity

Key Points - National Cybersecurity Alliance govt. – industry initiative to increase safety online
- National media campaign ‘Stop – Think – Click’
- Working on Boot camp for Cyber security
- Taking security out of the high risk end user environment – Schools – SME’s
- Chance of a virus attack quoted as 7 in 10 users

Peter Lübkert
peter.lubkert@oecd.org
Head of Division within the OECD Directorate for Information Technology and Network Services

Addressing Information Security Needs of Users – Practical experience at the OECD
- Key Points - An Operational view following ISO 17799
- Security and Costs are an issue
- Perimeter one line of defence but only the first
- Too many security passwords leads to risks
- Patch dilemma for large groups let alone SME’s and Individuals.
- Emerging technologies – Self healings systems/devices; System pattern monitors based on defined user patterns
APEC-OECD Workshop on the Security of Information Systems and Networks
6-7 September 2005, Seoul, Korea

Michael Mudd,
Director of Public Policy, Asia - Pacific
The Computing Technology Industry Association - CompTIA®
mmudd@comptia.org

©2005 CompTIA
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION