Addressing Information Security Needs of Users - Practical Experience at the OECD

Objectives

» Illustrate the complexity and challenges of establishing and keeping secure ICT environments

» Highlight a few essential aspects of operational ICT security
Where are we going?

» The dimension/nature of the issue is changing
» From “hacking for fun” to well organised and often targeted attacks
» Complex interrelations between application software (packages) and security tools

In other words – it is getting more and more difficult!

Security at the OECD Secretariat

Our operational security follows the principles of the OECD guidelines + ISO 17799

» Work with users – awareness / responsibility
» Ensure business continuity – response / contingency
» Engineering design / implementation / management
» OECD Risk Register – risk (re)-assessment
» OECD privacy commission – ethics / democracy

Proportionality is an important aspect, not to forget costs
Levels of protection

» Perimeter defence alone is not enough
» Application security, access control and identity management matter
» Network and information transmission security are necessary
» End-user/device security

End-Point Security

» Corporate client security
  » Personal firewalls
  » VPN (IPSec & SSL)
  » Authentication, authorization, and centralised administration
  » Secure messaging
  » Spam and Web filtering
  » Anti-virus and spyware protection
And yet ...

» Multiple security layers
» Strong passwords, pass-phrases
» Etc. … →

Too many/complicated solutions may have the opposite effect (security vs. convenience)

Security Solutions

» Security tools have to address various constituencies with different needs/means:
   » Businesses and governments
   » Consumers and citizens
» The value of information has to be understood (information risk management)
» Privacy and trust are important issues
» Ease of use and simplicity are paramount
**Some challenges ...**

- Threats are silent and non-visible
- There is more and more hidden infrastructure (devices and services)
- People – are the easiest target and weakest security link (social engineering)
- Raising security awareness among end-users is important but not enough
- Building trust is essential
- Costs – security doesn’t come free

**A security framework ...**

- Management support
- Appropriate technology
- Collaboration and trust
- Policies and guidelines
- Contingency plans / audit ...

*OK for the enterprise but what about the individual user/consumer or even the very small business?*
Technical support - Keeping IT up-to-date

» The complexity of and interaction between business applications and security tools pose a constant functional risk
» Technological evolution/change management
» The “patch” dilemma/collision
  » You cannot ignore them
  » Can you trust them, how do you test them
  » Apply them not too early but before it’s too late

Even professional ICT support groups struggle ...

Some avenues to explore

» Offer new services (to support consumers)
» Work with software vendors towards integration of tools instead of best-of-bread approach
» Don’t rush software developments/upgrades
» Ensure that the return on ICT security investments is well understood
» Business alignment → consumer alignment
Emerging technologies

» Self-healing systems/devices
» Small routers with integrated security features
» Use of behavioural analysis tools instead of traditional end-user security software
  » On the desktop (alert)
  » As a means to identify fraud based on client profile information (alert)
» …

For discussion …

» (How) can simple security be achieved fast?
» How to foster a “culture of security” on the end-user/consumer level?
» Solutions often look simple on paper but can they always be implemented?
» Budgets and costs – how to sustain security spend?