CSIRTs and ISO/IEC

- ISO/IEC Background
- ISO/IEC Engagement Process
- History: ISO/IEC 18044
- Future: ISO/IEC 27035
- Discussion / Way Ahead
CSIRTs and ISO/IEC

**ISO/IEC Background**

- ISO/IEC Engagement Process
- History: ISO/IEC 18044
- Future: ISO/IEC 27035
- Discussion / Way Ahead

---

ISO/IEC Background (1)

- **International Organization for Standardization** (ISO)
  - *Organisation internationale de normalisation*
  - Founded 23 February 1947
  - Headquartered in Geneva, Switzerland
- International-standard-setting body composed of representatives from various national standards organizations.
- Promulgates world-wide industrial and commercial standards
- Although technically a non-governmental organization (NGO), it is consortium with strong links to governments, able to set standards that often become law, either through Treaties or National Standards
ISO/IEC Background (2)

• Most work in the Information and Communications Technology (ICT) arena is carried out in conjunction with the International Electrotechnical Commission (IEC), through Joint Technical Committee Number 1 (JTC1)
• IEC is a not-for-profit, non-governmental international standards and conformity assessment body for all fields of electrotechnology, founded in 1906
• IEC’s own documents in 6xxxx – 7xxxx number range

ISO/IEC Background (3)

• Within the ICT arena, the concerns of Information Security are predominantly handled by JTC1 Sub-Committee 27 (SC27)
• SC27 has led on the unification of a variety of differential Information Security standards under the ISO 27xxx series
  – For instance BS7799 became ISO17799 initially, but now is ISO27001
• However there are still some “orphans”
CSIRTs and ISO/IEC

- ISO/IEC Background

- ISO/IEC Engagement Process

  - History: ISO/IEC 18044
  - Future: ISO/IEC 27035
  - Discussion / Way Ahead

ISO/IEC Engagement Process

- Documents produced as:
  - Technical Reports
  - International Standards

- Documents normally generated by Projects, which are voluntary groupings consisting of:
  - Representatives from participating National Standards bodies
  - Additional Liaison Members from relevant communities of interest

- ISO/IEC ratification through Committees and Sub-Committees
CSIRTs and ISO/IEC

- ISO/IEC Background
- ISO/IEC Engagement Process

➢ History: ISO/IEC 18044

- Future: ISO/IEC 27035
- Discussion / Way Ahead

History: ISO/IEC 18044 (1)

- Full title
  - ISO/IEC TR 18044:2004
  - Information technology
    - Security techniques
      - Information security incident management
- Technical Report (TR)
- Published 12-Oct-2004
- Produced under ISO/IEC JTC1 SC27
History: ISO/IEC 18044 (2)

- **Objective:**
  - Provide advice and guidance on information security incident management for information security managers and for information system managers.
- **Contains:**
  - information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used)
  - information on examples of information security incidents, and an insight into their possible causes
  - a description of the planning and documentation required to introduce a good structured information security incident management approach
  - a description of the information security incident management process

CSIRTs and ISO/IEC

- ISO/IEC Background
- ISO/IEC Engagement Process
- History: ISO/IEC 18044
- **Future: ISO/IEC 27035**
- Discussion / Way Ahead
Future: ISO/IEC 27035

- Evolution of ISO/IEC TR 18044:2004
- Changes nature from Technical Report (TR) to International Standard (IS)
- Currently at Working Draft (WD) stage
- Planned for ratification at ISO/IEC JTC1 SC27 Plenary Meeting (October 2008, Cyprus)
- Concerns expressed by some CSIRT communities that haven’t been engaged in structured manner with either ISO/IEC 18044 or ISO/IEC 27035 (Draft)

CSIRTs and ISO/IEC

- ISO/IEC Background
- ISO/IEC Engagement Process
- History: ISO/IEC 18044
- Future: ISO/IEC 27035

➢ Discussion / Way Ahead
Discussion / Way Ahead

Possible Topics

– Documents
  • History with ISO/IEC 18044
  • Future with ISO/IEC 27035

– Engagement
  • Through National Bodies
  • As Project Liaisons
    – TF-CSIRT
    – Other Bodies (APCERT, EGC, ENISA, FIRST)

– Any Other Issues?

Contact Details

Ian Bryant
Information Assurance (IA) Projects Advisor
Defence Security Standards Organisation (DSSO)

UK Ministry of Defence (MOD)
Whitehall, London, SW1A 2HB, England

ibryant@relay.mod.uk
+44 20 7807 0352; Desk
+44 79 7312 1924; Mobile

www.mod.uk