National Infrastructure Security Co-ordination Centre

Peter Burnett
Head of Information Sharing
Background

- Late 70’s – Mainframes, Minis, Micros
- Languages
- Evaluation & Certification, CLEFs
- Compusec, Infosec
- CNI/CIP Programme
- CERT Management
- EU & Intnl Liaison
Information Sharing

What is it?

- ‘Incident Reporting’, +
  - Intrusions, Viruses, Observation, Tipoffs
- Warnings, Alerts etc, +
- Education/Awareness material, +
- Peer to Peer exchanges, networking, +
- Threat & vulnerability information, +
- Help, Advice,
- To improve Internet Security
Who is it?

- CIP Organisations (e.g. incl CESG) +
- Research Centres, Groups +
  - (e.g. SANS, EICAR, AVIEN)
- Vendors, AVS etc +
- ISACs ? +
- WARPss
  - Warning, Advice & Reporting Points
Who is it?

- Most important of all ….
- CERTs & CSIRTs
- Key to the whole network
- Already doing it.
  - RFC 2350
- The model for development.
UK CERT Involvement

- UNIRAS - Govt CERT since 1992
- Incorporated into CIP organisation
- Links to US/CAN/AUS/NZ
- European Govt CERTs Forum
- Participation in TF/CSIRT, FIRST
UK Initiatives

- UK CERTs forum
- Encouraging new CERTs in UK
- Encouraging Information Sharing Bodies
  - SAINT, ISACs
- Support for EU projects (CASES, EWIS etc)
- Conceive & promote WARP\Ps
  - Warning, Advice & Reporting Points
  - Linked to CyberHood Watch (IAAC)
Warning, Advice & Reporting Points (WARPs) - Functions

- Issue Alerts & **Warnings** from CERT/WARP network (and CASES)
- Act as helpdesk for **Advice** on Internet/Infosec problems
- Gather, sanitise, and *share* Incident **Reports** (with CERTs, WARP, CASES)
- Geared to SMEs, small organisations & Citizens
The WARP model

Information Sharing Network

WARP

Incident Reports
Problems

Warnings
Advice

e-COMMUNITY

Trade association, interest group, local authority, industry sector
Information Sharing

WARPs Approach

- Internet-based
  - Distributed (the Internet is not mainframe-based)
  - User-oriented (bottom-up)
  - Devolved (allows specialisation)

- Small is beautiful
  - In touch with community’s requirements
  - Builds trust through familiarity

- Builds on successful ideas
  - Neighbourhood Watch
  - Citizens Advice Bureaux
  - CERTs/CSIRTs
What do WARP\textsuperscript{S} do ?

- **Receive** warnings/advisories from WARP\textsuperscript{S}/CSIRT\textsuperscript{S}/CERT\textsuperscript{S} and other sources, filter and assess them, and **reissue** them to their community where appropriate, (perhaps with increased priority or added value).

- Provide Email and/or telephone **advice** to community members on security matters.

- **Solicit** and record IT-security incident **reports** from community.
– **Share** (possibly sanitised) *incident reporting data* with other WARPs/CERTs etc with whom a sharing agreement has been reached (formal or informal).

– **Contribute** incident data, resources and/or expertise/knowledge to peers etc to help deal with *widespread problems*.

– **Participate** in ‘networking’ and sharing of experiences and knowledge with other members of Information Sharing network

– **Develop** close links with selected WARPs/CSIRTs/CERTs for support and *collaboration* on problems.
WARPS – What DON’T they do?

• RESPONSE !!!
Objectives

• Increase Awareness, Education:
  – general e-environment (reduce Viruses, Worms, Trojans, DDoS etc)

• Provide useful and timely warnings

• Gather incident reports
  – Crime reports (pass on only with consent)
  – Statistics, Trends
  – Attack detection
CSIRTs & WARPks ?

• What’s in it for you ?
1. Your country needs more CSIRTs
2. WARPks are cheap & simple (relatively)
3. CSIRTs can increase their coverage, effectiveness and influence, at little cost
4. You can help SMEs, Citizens & others
5. We can improve the general environment
6. It’s an incident early warning system
CSIRTs & WARPs?

- What do they need from you?
  1. Acceptance/tolerance
  2. Advice on establishing themselves
  3. A feed of advisories etc
  4. Technical advice (if convenient)
  5. Trust (eventually)
  6. Someone to pass incident reports to, (with no obligation for Response)
CSIRTs & WARPSS?

- Think of WARPSS as:
  - Satellites
  - Sub-CSIRTs
  - Local branches
  - Nodes to help reach a wider audience
  - Something to fill the coverage gaps
  - Future CSIRTs?
  - Anything you like really!
CASES
Cyber-Awareness and Security Enhancement Structure

- A Coordinating Centre to encourage dissemination of Warning & Awareness materials via National Nodes
CASES – Transnational approach

- Builds on elements already there (CSIRTs, WARPks, e-Platforms)
- Provides Coordination i.e. Cooperation (not control)
- Aids e-Europe Programmes (confidence)
- Promotes new national nodes (where they don’t exist)
- Stimulates national Dissemination network, WARPks
- Complements R&D work (identifies needs)
- Provides test-bed
WARPs – A local approach

- Builds on elements already there
- Reflects Internet philosophy
- Cooperation not control
- Provides help & advice
  - Builds Trust
  - Builds Confidence
  - Builds an Incident Reporting network
Questions ?
Plain Sailing from now on ?
No such thing as Plain Sailing!