



IT Security Awareness for Everyone

Profiles for Warning Dissemination

Dave Freeman
ITsafe Service Team

21st TF-CSIRT Meeting
3rd May 2007, Praha CZ

Profiles for Warning Dissemination

- The Requirement
- The VEXWM
- Use of Method

Profiles for Warning Dissemination

► The Requirement

- The VEXWM
- Use of Method

Why a Rating System

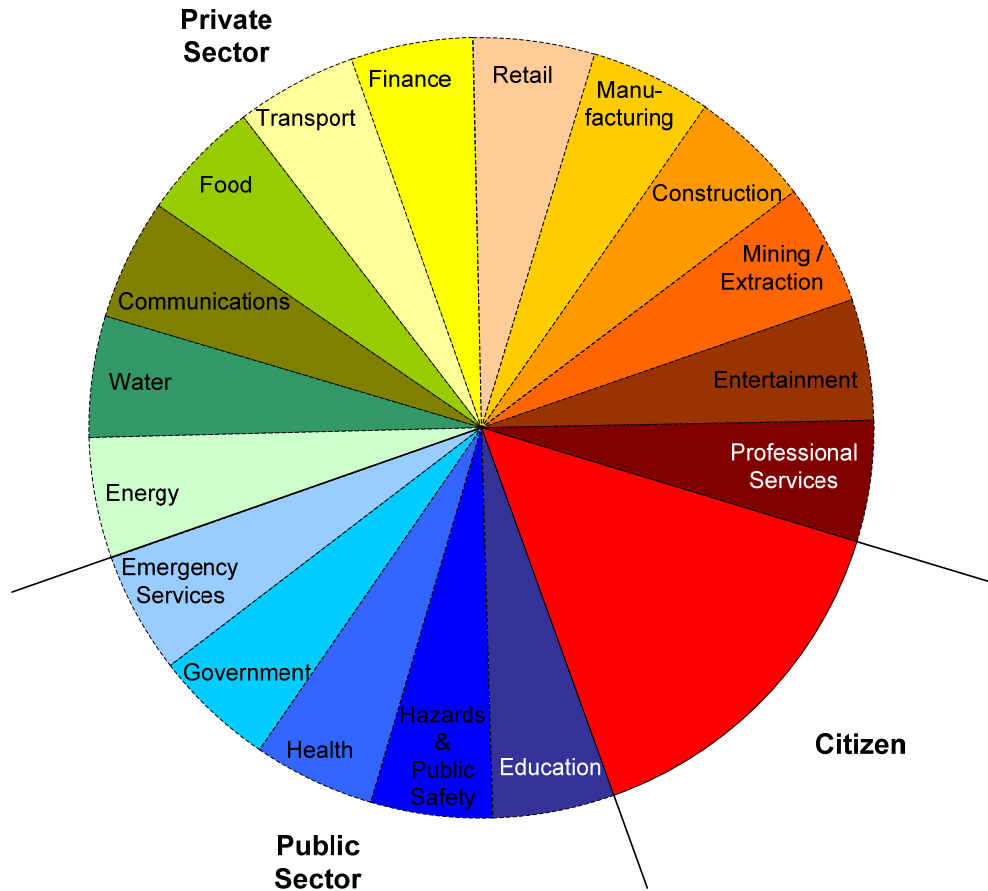
- Multitude of technical IT issues
 - Vulnerabilities
 - Exploits
 - Mis-configurations
 - Incompatible inter-relationships
- Need to prioritise
 - Severity of the Issue
 - Relevance to the customer base



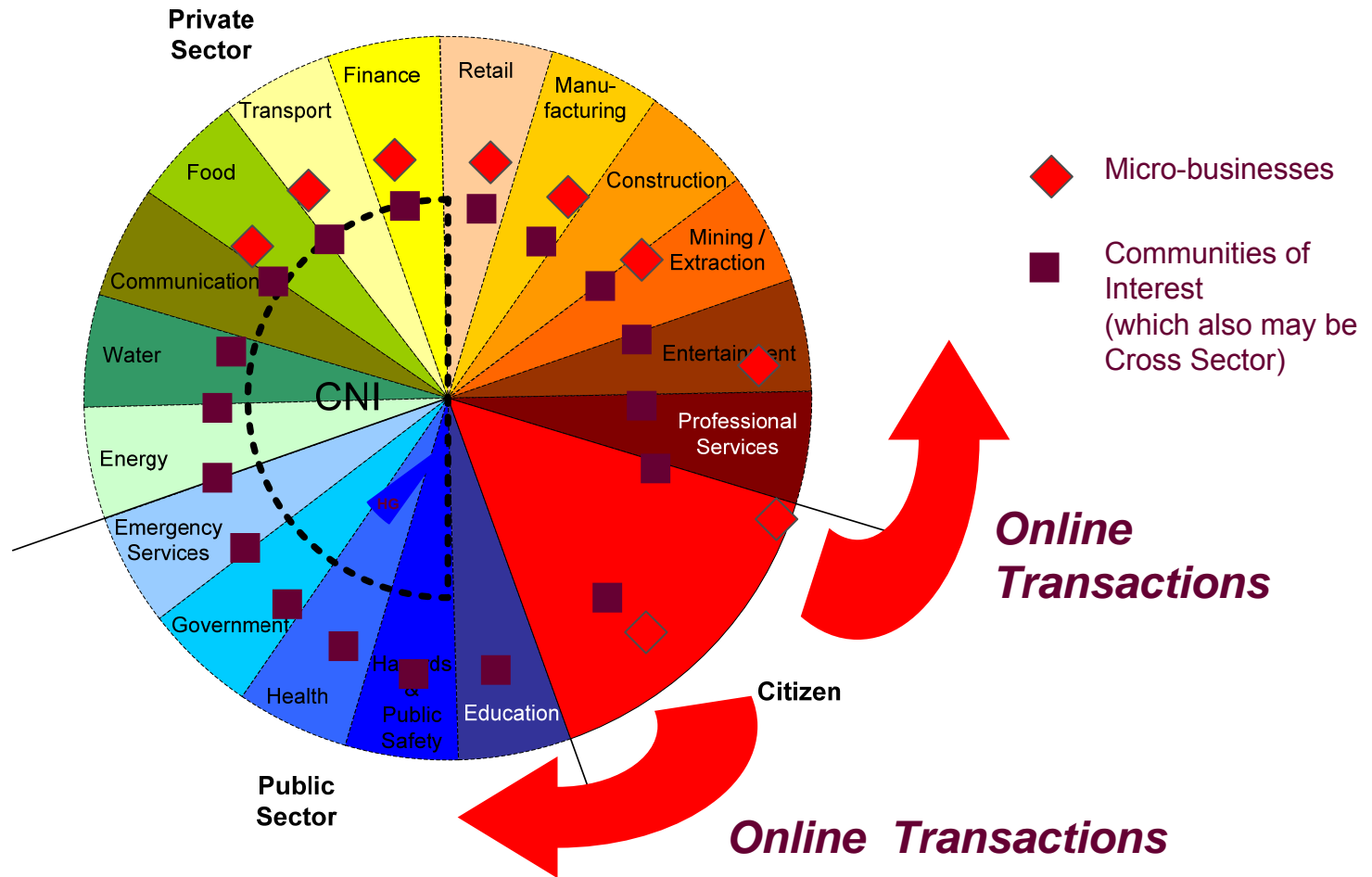
Types of Warning (e-Risks)

- **Vulnerabilities** - technical problems, of either an architectural, implementation or configuration nature, which would allow a malefactor to perform undesirable actions to a system
- **Exploits** - techniques used by malefactors to perform undesirable actions to a system, which may either be as a result of a new or changed Vulnerability, or by an unintended approach to a legitimate facility, typically a failure in non-technical Information Assurance (IA) countermeasures in the personnel, physical or procedural realms such as leaving a system logged in where unauthorised personnel could gain access

Sectoral View of the UK



Audience Groupings



Audience Characteristics

- Across, and within Sectors:
 - Differing levels of technical knowledge
 - Differing levels of technical interest
 - Differing hardware platforms
- These characteristics can be used to Profile the Warning Services needed, e.g.
 - Full technical feeds for Major Corporates
 - Plain English, heavily filtered feeds for Citizens and Small Businesses

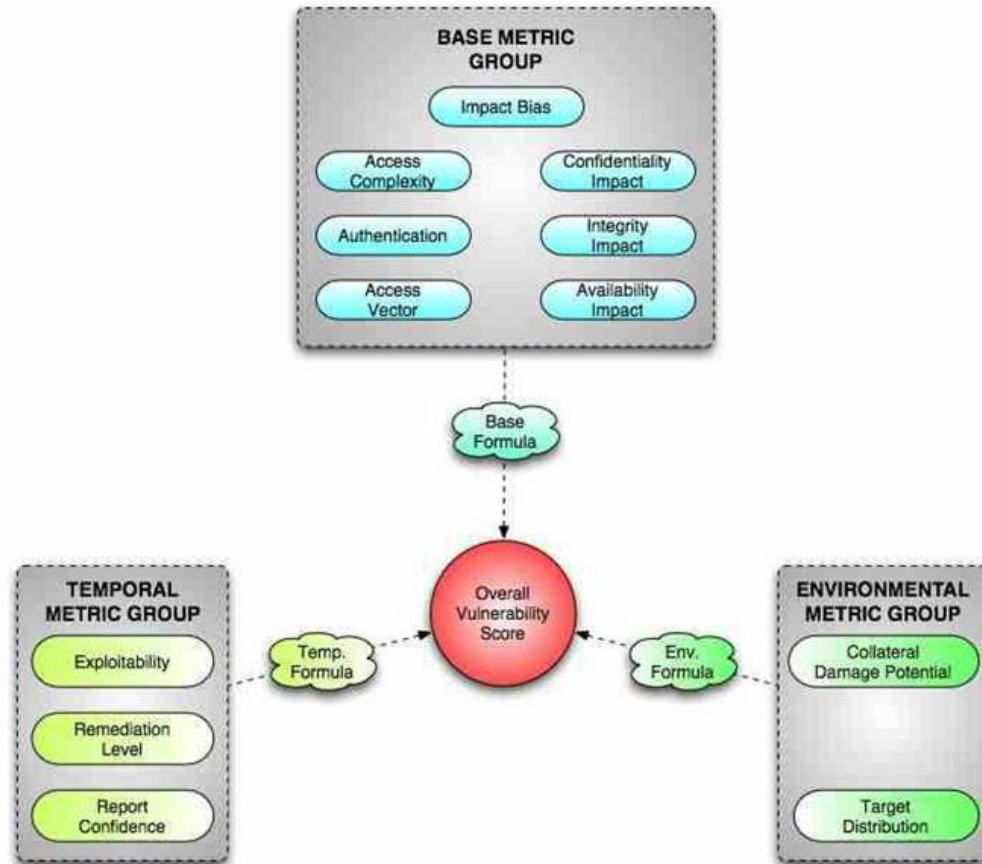
Profiles for Warning Dissemination

- The Requirement

▶ The VEXWM

- Use of Method

Possible Answer – CVSS (1)



Possible Answer – CVSS (2)

- Common Vulnerability Scoring System (CVSS) developed on behalf of the US National Infrastructure Advisory Council (NIAC)
 - Now under the stewardship of Federation of Incident Response Security Teams (FIRST).
- Uses a Base score and two Context scores (Temporal and Environmental) to allow localisation.
- Despite localisation, widespread mis-understanding that there is a single “CVSS answer”.
- Some parameters within the Base assessment more suited to a Context view
 - Impact is inconsistent with a genericised abstraction, as this will normally be audience specific.
- Does not currently meet UK needs for customised, measurable and replicable Triage.

VEXWM

- Vulnerability and Exploit Extensible Weighting Metric
- Optimised so that input parameters are objective in nature to maximise replicability when used by different operators
 - Accept these parameters are only Nominal or Ordinal measures of reality
- Extensible so can be used either in environments where differing information needs exist within and between the customer base, or to share the common base data amongst differing organisations
- This is implemented by the provision of Profiles for each relevant scoring element, and the final outcome of the metric will be one or more Profile Scores relevant to the particular usage(s).

VEXWM Structure

- Founded upon 5 Parameter Groups:
 - Adversity Category
 - Platform Type
 - Potential Damage
 - Remediation Difficulty
 - Community Prevalence
- Underlying formula based on logarithmic addition, as this has the following desirable properties:
 - Reduces “order of magnitude” issues to manageable proportions
 - Avoids “multiply by zero” issues

Adversity Category

Adversity is used rather than Threat (actions with intent), as this includes also Hazards (issues based upon a probability of occurrence)

- Hazard-Environment (e.g. localised Denial of Service (DOS) from a bearer having bandwidth consumed by attack elsewhere)
- Hazard-WIMP (Well Intentioned but Misguided People – e.g. falling victim to social engineering)
- Hazard-MalWare
- Threat-Hack
- Threat-Crime
- Threat-ESA (Empowered Small Agents)
- Threat-Nation (i.e. acts of war)
- No-Threat-Hazard

Platform Type

- Hardware
- Firmware
- Microcode
- Operating System
- Middleware
- Net Enabled Software
- Security Software
- Other Application

Potential Damage

Category, modified by Virulence and Duration

- Modify/Delete
- Bearer DOS
- Host DoS
- Potential Remote Modify
- Potential Remote View
- Other Visible
- Local Modify/View
- Social Engineering
- None

Remediation Difficulty

- Warning Type
 - Active / Current / Imminent / Future
- Confidence Modifier
 - Trusted / Known / Unknown
- Fix availability (whether the fix is already available, or when it is likely to be so)
 - Future >24 Hours / Future <24 Hours / Current / Historic
- Type of Fix - how approach is applicable and/or understandable to the Target Audience(s)
 - None / Manual / Outline / Script / Signature / Patch / Automatic

Community Prevalence

- ICT Stack represented as 4 component groupings:
 - Hardware
 - Operating System
 - Net Enabled Software
 - Other Application
- Each Community has weighted profile for major ICT
 - Currently derived from CMSI
 - Looking at CPE

Profiles for Warning Dissemination

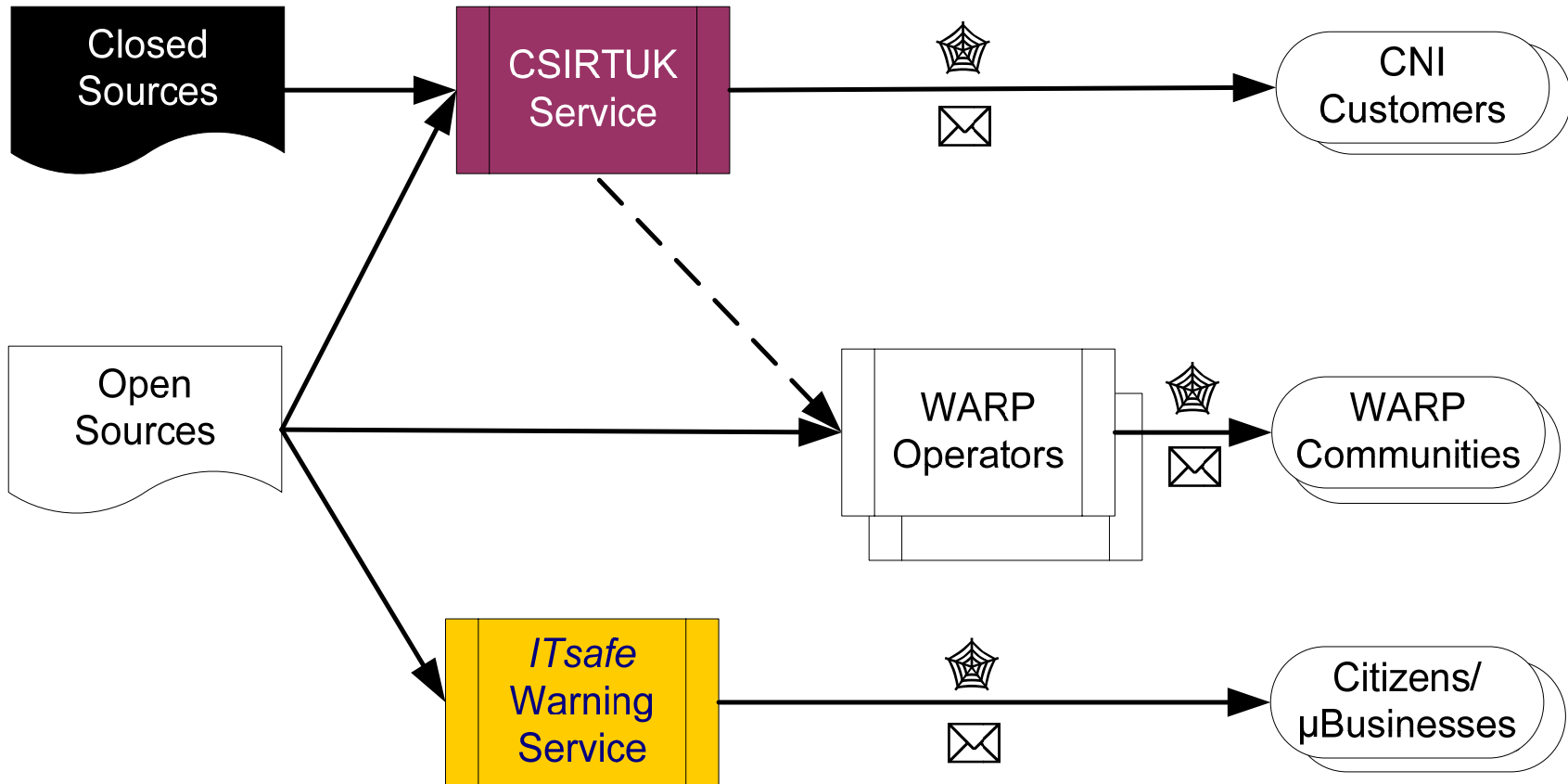
- The Requirement
 - The VEXWM
- **Use of Method**

ITsafe and GetSafeOnline

- ***ITsafe*** is a service, launched on 23rd February 2005 by Home Office Minister Hazel Blears MP, to provide Plain Language Warnings to Micro-Businesses and Private Citizens in the UK
- ***GetSafeOnline*** is a Public / Private initiative, working in partnership with the *ITsafe* Warning Service, to provide a source of information and good practice to Micro-Businesses and Private Citizens in the UK



Current UK Warning Information Flows



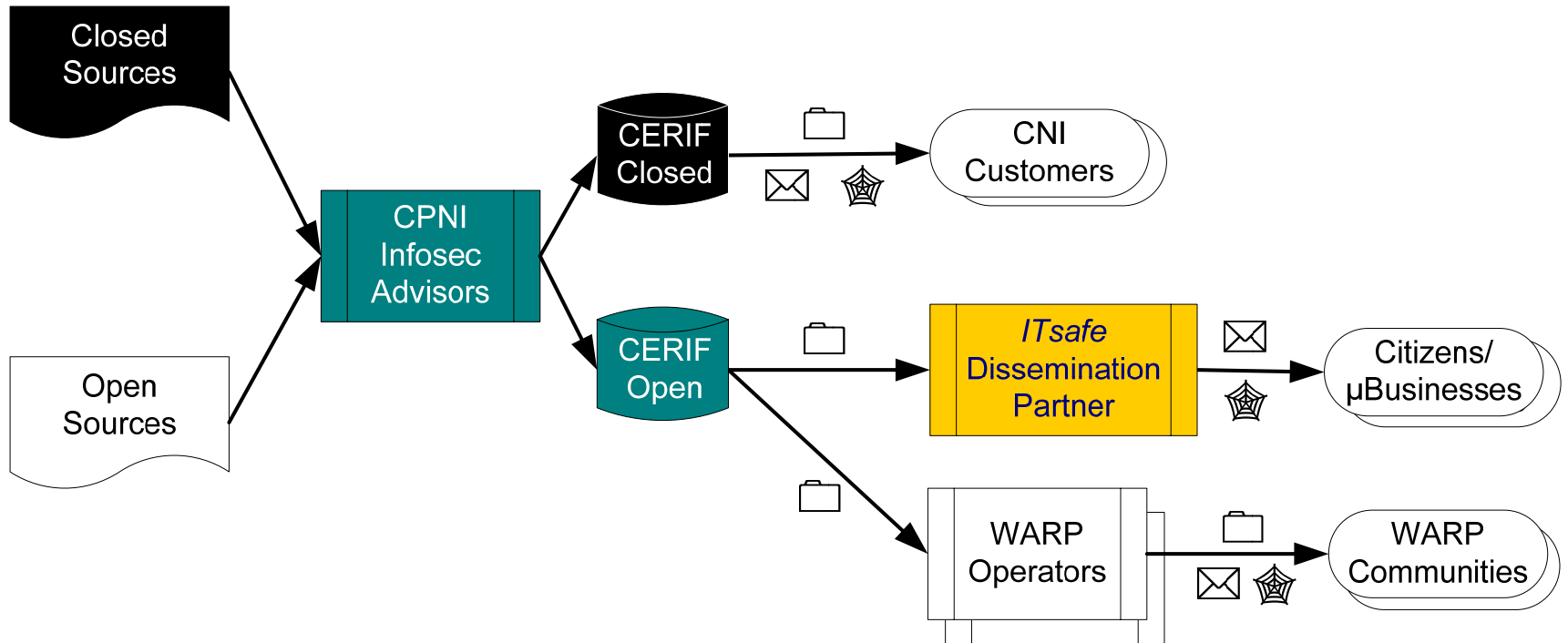
Current version of VEXWM has been in Prototype use by ITsafe since February 2007

Use of VEXWM

- Prototype being used by ITsafe since February 2007 with a Citizen focussed Profile
- GetSafeOnline will launch a service aimed at SME's at the end of June 2007 using VEXWM with a SME focussed Profile
- Discussions underway with Australia for UK to provide a VEXWM based feed employing a Profile supplied by Australia



Future UK Warning Information Flows



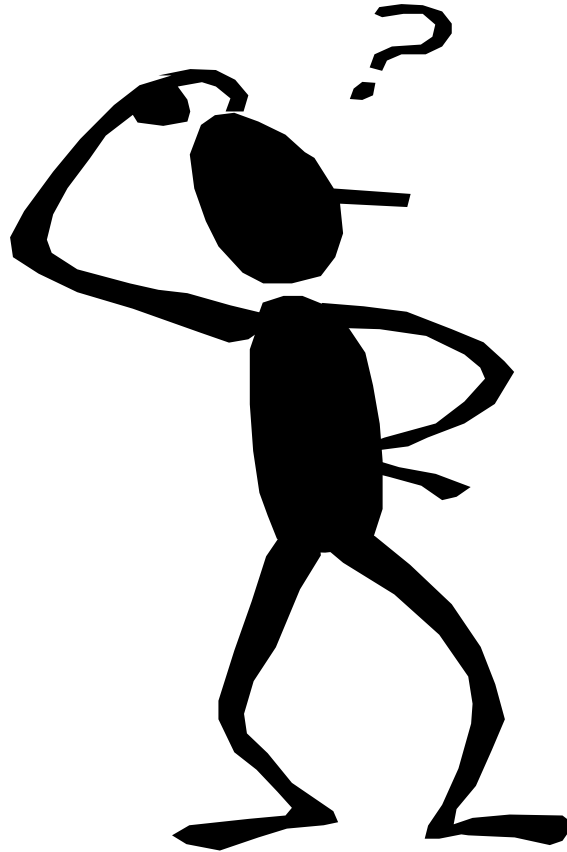
CPNI e-Risk Information Feeds (CERIF)

- Based on Extensible Markup Language (XML)
- Initial offering will have 4 variants :
 - A Document Object Model (DOM) replication of the full, analysed, Vulnerability or Exploit CERIF records
 - An RSS “Ticker” pointing to the CERIF record
 - A “rich” RSS Ticker derived from the VEXWM profile for the ITsafe Citizen Audience, and containing Plain Language subset of CERIF record
 - A “rich” RSS Ticker derived from the VEXWM profile for the GetSafeOnline Small Business Audience, and containing Plain Language subset of CERIF record

CERIF Elements

- Generic Dublin Core (DC) Metadata fields
- Generic e-Government Metadata Standard (eGMS) fields
- Data Labelling Namespace (DL-NS) fields
- Interim Vulnerability and exploit Description and exchange Format (IVDF) fields
- Information and Communications Technology Namespace (ICT-NS) fields
- Fields to support profiling of outputs

Questions ?



Contact Details

Ian Bryant

Dave Freeman

ITsafe Service Team

2nd Floor Ripley Block, 26 Whitehall
London, SW1A 2WH, England

+44-87-0114-4561

Telephone

+44-87-0114-4546

+44-20-7276-5096

Facsimile

+44-20-7276-5096

Internet

hd-tech@itsafe.gov.uk

davef@itsafe.gov.uk

<http://www.itsafe.gov.uk>