

WARP SERVICES



Three core WARP services

Filtered Warnings Service

The Filtered Warnings Service allows WARP members to receive warnings and advisories that are filtered based upon their area of interest. The Filtered Warnings Application (FWA) software uses a subscription tree 'tick list' which allows WARP members to easily modify and maintain their selections. The software also helps WARP operators to easily categorise and distribute warnings and advisories in a timely manner. This service delivers the **Warning** part of the Warning, Advice and Reporting Point.

Advice Brokering Service

This service allows WARP community members to discuss good practice and information security issues in a secure environment. The service also enables members to offer their experience and skills to others, possibly on a barter basis, where one has done work in an area that another is contemplating. This service delivers the **Advice** part of the Warning, Advice and Reporting Point.

Trusted Sharing Service

This service provides a trusted environment in which WARP members can share sensitive information, such as incident or threat data, in the knowledge that it will not cause them harm or embarrassment. Reporting can be achieved via the telephone, email or face-to-face, with appropriate security safeguards. Once sanitised, and anonymised if appropriate, such incident information may also be passed to other WARPs with whom a trusted relationship exists, and to NISCC, for collating and monitoring national trends. This service delivers the **Reporting** part of the Warning, Advice and Reporting Point.

Subscription Tree

Please select the categories of interest to you below, you can select as many as you like, simply tick the branch and all the sub-items will be selected. Commit your changes.

This means there are one or more items selected below this branch.

This item has been selected but you have not yet saved your changes

- All Categories
- Good Practice
- Incident/Threat
- Vulnerabilities/Fixes
- Cisco
- HP
- Linux/Apache
 - Apache
 - Debian
 - Mandrake
 - RedHat
 - SuSE
- Microsoft
 - MS Bundled Windows Software
 - MS Developer Products
 - MS DirectX SDK
 - MS Visual Studio
 - MS Office/Business Products
 - MS Home Products
 - MS Server Products
 - MS Windows Operating Systems
- Sun Microsystems
- Apple

RUNNING A WARP



Code of Practice

The WARP Code of Practice is designed to ensure that WARPs conduct their business in a responsible manner consistent with a set of values which engenders trust. This trust is important not just within the WARP's own community, but also within the broader WARP community.

WARP vision

WARPs are part of NISCC's information sharing strategy. WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting. Membership of a WARP can also reduce the costs of good security. WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised and therefore reduce the risk to their organisation. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business sense.

Responsibilities of running a WARP

- WARPs will use the WARP name, logo and brand, in a responsible manner.
- WARPs will seek to promote the establishment of further WARPs as required.
- WARPs will contribute freely to the WARP Toolbox any examples of good practice they develop for their WARP that are likely to be of benefit to other WARPs.
- WARPs will cooperate with, and support, other WARPs, and will make reasonable efforts to attend WARP forums.
- WARPs will not compete aggressively against other WARPs, nor try to prevent the establishment of new WARPs.
- Members of one WARP will not be prevented or discouraged from joining additional WARPs.

Incident Reporting

- WARPs will work to establish a trusted relationship with each of their members, to encourage Reporting.
- Subject to anonymisation, confidentiality, and resource constraints, WARPs will share with NISCC and other WARPs, any incident reporting likely to be of interest.

Governance

- WARPs will be run on a not-for-profit or cost recovery basis.
- WARPs will ensure that their growth is constrained so that they do not reduce their effectiveness or quality of service to individual members.
- WARPs will not intentionally do anything to bring NISCC, the WARP model, brand or principles into disrepute.

Setting up a WARP?

The WARP registration case-study is **essential reading**. Find it on the WARP website.