

An Information Sharing Vision to improve Internet Security

This paper describes the long-term vision of an [Information Sharing Network](#), incorporating a new entity, the [WARP](#) ([W](#)arning, [A](#)dvice & [R](#)eporting [P](#)oint), alongside the established entities of [CERTs](#), and [ISACs](#). Some of the terminology is explained at [Annex A](#).

The WARP Concept

Overview

There is a need to establish a ‘network’ across the UK, linked to other European and worldwide networks, to provide better & more timely advice & warnings relating to [Electronic Attack](#) (EA), and for receiving incident reports. These will inform threat assessments, provide statistical data, and identify trends and new vulnerabilities. Although some elements of this network (e.g. a number of [CERTs](#)) already exist, and are connected (through the [TF-CSIRT](#) forum etc) they only serve a small fraction of Internet users, and are limited to specific communities, which are often already well-resourced. The WARP concept is designed to plug the gaps cost effectively. This is not a specific physical comms network (like the Internet), but more a grouping of organisations with a shared interest (who will of course be able to communicate). This should extend to all Internet users, from central and local Government, to large corporations, SMEs and home-users. Since central government and large corporations are generally well catered for already, this initiative focuses on a way of extending this service to others, particularly SMEs, regional and local authorities, and to home users. The mechanism proposed to assist this process is a small cost-effective unit, based on the concept of a [CERT](#), called a [WARP](#).

The Network

The long-term vision is for a network of WARPs and similar units, each communicating with many others. WARPs would deal directly (through formal or informal trust relationships) and with relevant centres of excellence (e.g. as mailing-list subscribers) forming an Information Sharing Network. This network would connect (at least indirectly) to all other WARPs and to CERTs, ISACs and technical advice centres.

The Units and their Communities

Each unit (WARP, CERT, [ISAC](#) etc) in the network would serve a community (see [diagram](#)).

- CERTs normally have a defined community for Response services at least, and a broader community for their advice (usually web-based).

- ISACs tend to be closed to information sharing beyond their own subscribers except through specific agreements, (but this may change, and may not apply to all ISACs).

All are concerned with passing on warnings etc to their communities, and receiving incident reports from their communities (and other sources). Other units may be interested in one or both activities.

- [CIP organisations](#) are interested in receiving incident reports, and may issue warnings, especially of very serious threats.
- [AVS](#) organisations issue advice and patches to their products for detecting viruses, and are also interested in reports of new viruses.

They all have something to gain from and/or contribute to being part of this Information Sharing network.

WARPs would each serve their own community of Internet users, the scope and constitution of which, would often be determined by the WARP's funding model, Commercial, Corporate or Cooperative/Public.

- Commercial, any paying subscriber would be a member.
- Corporate WARPs could be set up by large organisations for their staff or customers.
- Publicly or cooperatively funded, the funding source would determine the boundaries of the community.

A community could be:

- **geographically** based (e.g. if local-authority funded, or a local business group),
- **virtual** (non-geographic) grouping (e.g. special interest groups such as disabled users nationwide),
- based on a **functional** group (e.g. trade groups such as farmers, educational consultants, independent breweries etc),
- a service provided for **customers** (e.g. online banking customers).

Members of each community could 'subscribe' to several WARPs if desired (e.g. local geographic, customer, and special-interest virtual).

A community may be homogeneous in terms of its members' skill levels, or might comprise a full range of levels of expertise from the most uninformed home user to self-taught or professional experts (who could be encouraged to assist the WARP). The common factors would be Internet access, and a perceived requirement for Internet-related security advice and awareness.

A key feature of a successful WARP is that its staff will be very **familiar** with the needs, capabilities and problems of their community. They should be aware of the most commonly used hardware and (especially) software used by the community, and should develop particular expertise in the security issues relating to any community-specific software or hardware. For example, a WARP for farmers should be well up to speed with releases and problems relating to DEFRA-issued software, and should have an awareness of IT-related crime that targets farming communities. It is important to many users that they are not flooded by information of no concern to them, so a WARP would be expected to **filter** any warnings or alerts etc which they issued, to minimise the volume, and to **highlight** those of particular relevance and urgency to their community.

Such familiarity will not only increase the effectiveness of advice and warnings, but is more likely to engender trust, which will in turn stimulate incident reporting. Furthermore, the WARP would be expected to **sanitise** any incident reports before passing them on to other trusted nodes in the network, and to keep any identifying particulars strictly confidential.

Functions

Each WARP would be expected to carry out the following functions:

- ❑ Receive warnings/advisories from other WARPs/CERTs and other sources, filter and assess them, and reissue them to their community where appropriate, perhaps with increased priority.
- ❑ Provide e-mail and/or telephone advice to community members on Internet-related security matters.
- ❑ Solicit and record IT-security incident reports from community.
- ❑ Share (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 other network nodes to help deal with widespread problems.
- ❑ Participate in 'networking' and sharing of experiences and knowledge with other network nodes.
- ❑ Develop close links with selected WARPs/CERTs for support and collaboration on problems.

Resources & Staffing

- A WARP could be run by two staff each on a part-time basis, but ideally, there would be three or more staff, on a part-time basis, for resilience and serious incidents.
- The team would need good technical knowledge of Internet, PC hardware and software, malicious code, Information Security, any specialised hardware or software used by the WARP's community
- Incident handling skills would be needed to provide a minimal level of response to user problems with technical advice and to liaise with peer organisations for assistance or to assess warnings and reports; team members should be adept at dealing with telephone queries.
- The team may also be distributed, running the WARP on a job-sharing basis alongside other roles, possibly at different locations. They would need good access to the following technical facilities, which may also be distributed:

Essential:

- Internet Browsing (2 or 3 terminals, at least 1 standalone)
- Email sending & receiving (several accounts with at least 2 ISPs using different backbone providers if possible)
- Several telephone lines
- Up to date Windows OS (2000, NT or XP) plus Mail programme.

- Encryption/digital signature capability (e.g. PGP) for exchange of information with community and other WARPs etc as necessary
- Backup facilities

Desirable:

- Standalone research machine with UNIX/LINUX & other OSs (exchangeable)
- Fax, mobile phones, pagers, laptops.
- Training budget.

Other considerations:

- Out-of-hours cover could be provided by a combination of on-call home-working and diversion of enquiries to another WARP/CERT with greater resources and out-of-hours coverage.
- Partnerships with industry or universities may supplement the knowledge & experience of a WARP.

Funding

- Commercial
 - A CERT service could be contracted from a commercial provider, but is likely to be expensive and less personalised than a locally managed unit. Some companies in the UK and elsewhere provide such services, (often under the CERT name) though they do not engage significantly in information sharing.
- Customer
 - A large organisation or group may provide this service to its customers (for a minimal charge or free) in order to encourage use of its on-line services (e.g. banking), to improve consumer confidence, and for the public good to increase awareness and education.
- Public-Private
 - A joint public-private funding arrangement might be possible with an organisation that has some of the necessary technical expertise or other resources, and is willing to assist for the common good.
- Corporate
 - This is the simplest model, with a large organisation providing the service to its staff. This model is used by some large organisations in the IT and Telecoms fields, but could be used by an enlightened organisation wishing to improve its staff's IT literacy or protect its IT users. In some cases, this could simply be an extension of an IT help desk, but would need to be extended to involve interaction with other WARPs on information-sharing.
- Cooperative
 - In many ways, the optimum arrangement is cooperative funding from subscriptions by the members of the community (possibly supplemented from public funds or corporate donors). This is likely to increase 'buy-in' from community members, and should assure trust in confidential handling of incident reports.

Peer relationships

The vision is that all WARPs, and most CERTs and ISACs and other related bodies will one day be linked in a network that can rapidly warn of new & serious viruses, Internet worms, or other attacks.

Each WARP will normally filter all warnings received, for duplication, integrity, and relevance to their community, and they may be able to add value from their technical expertise and knowledge of community systems.

The network would also facilitate the speedy upward and lateral dissemination of incident report data, to WARP/CERT peers with whom there is an information sharing agreement, including any WARPs/CERTs etc performing a collation and assessment function.

Individual judgement and trust issues arise here. These can be addressed by means of WARP workshops and discussion fora. It is expected that most WARPs will develop links with a handful of other WARPs, with whom they feel comfortable, and can share trust, and with whom they will share incident reports for mutual benefit. They may also develop a wider circle of links with other network nodes whose judgement and integrity they trust when receiving warnings, and to whom they may send serious incident reports (if not routine ones). This mirrors the [FIRST](#) network to some extent, which has informal sub-nets of trusted members.

Why NISCC is supporting WARPs

It is important for NISCC to encourage and foster the development of WARPs in the UK and across Europe, for several reasons:

- NISCC needs to focus on its primary community, (Central Government and the CNI) but can share its information more widely, knowing that its warnings will be intelligently filtered and disseminated by WARPs.
- It needs channels and mechanisms in place to disseminate warnings as quickly and widely as possible; WARPs will provide channels to their communities.
- It is important that all users of the Internet are as security-aware as reasonably possible to reduce the impact of widespread attacks (such as major viruses, worms, DDoS etc) that exploit mass user connectivity; WARPS can help educate their communities.
- NISCC needs as much incident reporting as possible from across the UK and elsewhere in order to be able to accurately assess the threat, and detect and react to serious electronic attacks against UK interests; WARPs can supply incident reports, perhaps uniquely, from their communities.

What NISCC will do to support & promote WARPs

Through UNIRAS, the UK Government CERT, NISCC will assist WARPs to establish themselves, by drawing on its knowledge, experience and contacts. In particular UNIRAS:

- has a great deal of experience in running what is in effect a WARP
- has been active in promoting the concept of WARPs/CERTs in Europe through the TF-CSIRT initiative
- is very well-connected with other major CERTs in FIRST and elsewhere
- has a good reputation amongst its community and peers for reliable warnings/advisories
- has a good track record in maintaining confidentiality of incident reports
- has fostered particularly good links with existing CERTs in the UK through its UK-CERTs Forum
- is part of NISCC which can bring significant resources to the promotion and fostering of WARPs in the UK and Europe
- through NISCC, has access to sources of warning information that may not be available to other CERTs or WARPs in the UK or elsewhere.

NISCC will make this experience available to new WARPs, through visits and consultation, and will help them to build links with other CERTs and WARPs.

IT is important to the UK's policy of promoting Internet access and on-line services, and for the CNI protection programme, that UK WARPs provide coverage of our community effectively. This will help to provide the best possible service of warnings to the UK's CNI and to the rest of the population.

For further information on WARPs or NISCC's Information Sharing Strategy, please contact:

Head of Information Sharing, NISCC

at

enquiries@nisc.gov.uk

Glossary of Terms

AVS	Anti-Virus Software houses, e.g. Sophos, NAI, McAfee etc
CERT	Computer Emergency Response Team, trademarked term by CERT Coordination Centre (CERT/CC) the first and possibly biggest CERT, run by Carnegie Mellon University in US, with some US government support
CSIRT	Computer Security Incident Response Team, same as a CERT, but term favoured in Europe.
CIP organisations	Critical Infrastructure Protection organisations, e.g. NISCC, NIPC(U.S.)
EA	Electronic Attack (Hacking, Viruses, Worms, Trojans, DDoS etc), usually from external sources, though can be 'insider'. Similar to CNA – Computer Network Attack
FIRST	Forum of Incident Response and Security Teams – the global organisation to which most major CERTs subscribe. See www.first.org
Incident reports	These will often take the form of 'problems' or 'observations' reported to a helpdesk (in a WARP or CERT). They may be passed on to other nodes subject to sanitisation, anonymisation, permission and trust between those nodes. They may be passed on to Police with the sender's permission, or the sanitised intelligence might be passed on unattributably.
ISAC	Information Sharing & Analysis Centre. Conceived in US under PDD63 (1998) for incident reporting & alerting between organisations in each CNI sector (Energy, Finance etc). Many currently run by one US commercial firm, (except IT & Telecomms ISACs). Most ISACs do not normally share reports outside their own (paying) membership.
TF-CSIRT	Task-Force CSIRT (Computer Security Incident Response Teams – an alternative name for CERTs) which aims to unite European CERTs and influence EU policy; led by Terena, a European Academic and Research organisation based in the Netherlands. See WWW.terena.nl
Information Sharing Network	Loose voluntary linkage (not a technical comms network) of entities including CERTs, WARPs, ISACs, and other organisations interested in sharing warnings, vulnerabilities, threats and incident reports, and providing advice to each other and to their own 'communities'.
UNIRAS	UK Government CERT, now part of NISCC.
WARP	Warning, Advice & Reporting Point. Provides a Warning, Advice and Reporting services on Internet security-related matters. Similar to a CERT, but without a capability for responding to incidents (other than providing advice).

WARP diagram

