

Serious about WARPs

2nd Annual WARP Forum

On Wednesday 15th March 2006 NISCC hosted the second annual WARP (Warning, Advice and Reporting Point) Forum. The event took place in London and was attended by delegates from across the globe including Estonia, Italy, Lithuania, Switzerland and the Netherlands. Experience ranged from representatives of existing and successful WARPs, to delegates who were learning about the initiative for the first time. This full-day forum offered delegates the opportunity to share advice and experiences with WARP colleagues, within a networking, presentation and workshop environment.



Timetable

The timetable for the day was as follows:

- | | | |
|-------|--|---|
| 10:00 | <u>Introduction & Aims of the Forum Latest Developments update</u> | Judy Baker, D/Director NISCC
Peter Burnett |
| 10:15 | <u>Keynote: WARP Prospects</u> | Alan Paller, Director SANS |
| 10:45 | AM Workshops ‘Sales Pitches’ | Co-Chairs
promoting their workshops |
| 11:20 | Morning Workshops | |
| | <u>Workshop 1</u> | WARPs and e-government |
| | Co-chairs | Bruno Brunskill and Judy Revell |
| | <u>Workshop 2</u> | Resilience-building with WARPs |
| | Co-chairs | Mick Humphrey and Mark Brett |
| | <u>Workshop 3</u> | WARPs in central government |
| | Co-chairs | Ian Dowdeswell and Andrew Powell |
| | <u>Workshop 4</u> | WARPs for SMEs |
| | Co-chairs | Geoff Smith and Jim Sunderland |
| | <u>Workshop 5</u> | International developments and CERT co-operation |
| | Co-chairs | Don Stikvoort and Mehis Hakkaja |
| 12:30 | PM Workshops ‘Sales Pitches’ | Co-Chairs
promoting their workshops |
| 14:00 | Afternoon Workshops | |
| | <u>Workshop 6</u> | WARPs and BS7799 |
| | Co-chairs | Natasha Stonestreet and Jim Sunderland |
| | <u>Workshop 7</u> | Education and health sector |
| | Co-chairs | Malcolm McKeating and David Harley |
| | <u>Workshop 8</u> | WARPs and e-crime/police |
| | Co-chairs | Mick Humphrey and Martin Wright |
| | <u>Workshop 9</u> | Partnerships for WARP development |
| | Co-chairs | Peter Daniel and Peter Kendal |
| | <u>Workshop 10</u> | Business benefits of WARPs |
| | Co-chairs | Bruno Brunskill and Diane Howorth |
| 15:30 | <u>Workshop Feedback</u> | Co-chairs
promoting their workshops |
| 16:30 | <u>Findings and Recommendations</u> | Alan Paller |
| 17:00 | <u>Final conclusions & Close</u> | Judy Baker |

Introduction and aims of the forum

The forum was opened by Deputy Director NISCC, Judy Baker.

Judy provided a brief overview of the development of the WARP programme since its inception in 2003. She described how the WARP project had grown since the 'birth' of the first WARPs in 2004. These original communities are now beginning to stand alone and act as a guide for potential new WARPs.

WARPs are growing in confidence and, whilst each group is different and uses the model to its own advantage, they all bring something new to the programme as a whole. These developments will lead to the anticipated maturity of the project, and the growth and spread of the WARP network. Judy encouraged existing WARPs to recruit new WARP champions – the more WARPs the stronger the model.

NISCC remains involved, facilitating events such as the WARP Forum and ensuring that the quality of the WARP brand is maintained. Most important is that *trust* remains key to this information sharing initiative and NISCC will work to ensure this.

Judy described the aims of the 2nd WARP Forum as helping newcomers to create new WARPs, sharing ideas and experiences so WARPs do not experience too many 'teenage problems' and helping WARPs to grow both nationally and across the globe.

Latest developments update

NISCC Head of Information Sharing and WARP project leader, Peter Burnett, then provided the forum with an update on the latest developments in the WARP initiative.

- There are currently 12 registered WARPs, 8 of which are operational and 4 of which are under development. There are a further 7 WARPs which are newly funded and 5 currently under discussion.
- Of the new WARPs the BTWARP provides services for small ISPs whilst a voluntary sector WARP has been set up with funding of just £200. This is a promising sign for groups wanting to set up WARPs on a minimum budget and demonstrates the flexibility of the WARP model.
- The emphasis for this year is to target education, central government and the voluntary sector. The project aims to have over 20 operational WARPs by close of 2006.
- WARPs are starting to go international, with interest expressed by a number of European countries as well as Australia, New Zealand and the USA.
- Developments in the Filtered Warning Application include a new developers toolkit as well as the production of an operators' manual. Uniras is to adopt the Filtered Warning Application software for its own work and it is hoped that other CERTs across central government will follow. Regular updates on this programme of work will be available from the WARP website www.warp.gov.uk

- The WARP model fits into one of ENISA’s four main work streams and the WARP programme will benefit from this. In particular ENISA is backing the WARP programme by providing a workshop and funding for the forum.

Peter concluded his presentation by emphasising the WARP vision. *WARPs will become endemic across the UK and beyond.* They will be self-replicating, free-standing and co-operating. They should improve the security of their members, the CNI and ultimately all IT users.

Keynote: WARP prospects



The forum keynote speech was provided by Alan Paller, Director of Research, SANS Institute. His presentation considered “Why do WARPs matter and how might they evolve?”

Alan suggested that WARPs matter because they:

- avoid duplication of effort and help communities to prioritise when dealing with security threats;
- develop trusted information sources – the longer a WARP successfully exists the deeper the trust among members; and
- develop trusted countermeasures for WARP members who do experience security issues – if information comes from a trusted source the recipient is more likely to act upon it as required for the good of the community.

Alan emphasised the importance of nurturing the trust developed amongst WARP communities - once broken it is difficult to regain.

Alan urged delegates to consider four key questions when evaluating the impact of their WARP:

1. How much threat did you remove for members in the past six months?
2. How much **more** threat can you remove for members in the next six months?
3. How much time did you save for members in the past six months?
4. How much **more** time can you save for members in the next six months?

By answering these questions honestly WARPs can evaluate their performance and consider how they might improve. It is important that the WARP model continues to evolve so it can be as useful as possible and not stagnate.

Alan also spoke about the relationship between WARPs and vendors. He commented that initiatives such as WARPs can influence developments in the vendor sector. One organisation alone cannot change the balance of power but a group of organisations, using similar software and seeking similar outcomes as exemplified by the WARP model has more power in the vendor/buyer relationship. WARPs should use their buying power to encourage vendors to ensure their products are as secure as possible.

Alan then provided the forum with a live demonstration of a cyber-attack and provided details of recently seen spear phishing attacks. This included an email which appears to come from the organisation's security officer and which directs the user to a website containing a bogus patch for a non-existent security issue. Alan encouraged WARP champions to stay current on new attacks in order to keep members informed and maintain trust levels.

To assist in this aim Alan recommended the following security websites:

- *SANS Information Security Reading Room*: Featuring over 1500 original computer security white papers in 71 different categories. <http://sans.org/rr/>
- *SANS Ouch! Security Digest*: A monthly security awareness report for end users. <http://sans.org/newsletters/ouch/>
- *Dshield.org*: A collation of cracker activity data from across the Internet. <http://dshield.org>

Workshop sessions

Two ten-minute sessions were then provided for co-chairs to 'sell' their workshops. Delegates attended two workshops of their choice during morning and afternoon sessions. The findings of all ten sessions were later fed back to the forum. Feedback was facilitated by Judy Baker, Peter Burnett and Alan Paller. Judy asked the co-chairs to provide comment on what they considered to be the most important issues to come out of the workshops.

Workshop One

Co-chairs

WARPs and e-government

Bruno Brunskill, Judy Revell

See workshop notes

Feedback session: The drivers for establishing WARPs within local government include meeting requirements of the ODPM 'take-up' campaign, Business Continuity Planning and security audits, expertise and resource sharing, efficiency and planned re-structuring. Successful WARPs can be developed from small, existing communities. It is useful to start small with the 'willing'. These groups can then be grown once benefits of the WARP can be tangibly shown. Management buy-in is important and can be encouraged by demonstrating the success of existing WARPs. It is difficult to encourage management to invest in a project without promise of results.

Workshop Two

Co-chairs

Resilience building with WARPs

Mark Brett, Mick Humphrey

See workshop notes

Feedback session: This group formulated the '4 Ps for WARP engagement':

People

Partnerships

Process

Practices

The forum agreed that TRUST is essential for the development of effective WARPs. They also emphasised the importance of people and partnerships for sustaining information sharing momentum.

It was commented that the WARP Toolbox is a useful tool for other partnership projects as it provides advice on methods, communication and information sharing.

Workshop Three

Co-chairs

WARPs in central government

Ian Dowdeswell, Andrew Powell

See workshop notes

Feedback session: WARPs in central government could help to raise the profile of IT security issues. There is a general apathy amongst staff that IT security is a 'techie problem'. WARPs could act as an 'outreach' facility for CERTs. If this relationship is to work effectively communication links between CERTs and WARPs must be in place. A system for measuring WARP effectiveness may also need to be in place.

Workshop Four

Co-chairs

WARPs for SMEs

Geoff Smith, Jim Sunderland

See workshop notes

Feedback session: The workshop agreed that the online business of Small and Medium Enterprises (SMEs) make them vulnerable to the activities of cyber criminals. WARPs can play an important role in protecting businesses from these risks.

The forum considered ways to make the SME community realise that these risks are real and that forming WARPs should be considered as part of their business strategy. SMEs need to be convinced that WARPs can bring measurable, financial benefits and that WARP communities can be formed without the risk of losing competitive edge.

It was also commented that WARPs could be used as a vehicle for promoting IT security advice within the SME sector and for building relationships between the SME 'vendors' and 'buyers'.

Workshop Five

Co-chairs

International Developments and CERT co-operation

Mehis Hakkaja, Don Stikvoort

See workshop notes

Feedback session: WARPs provide flexibility and better granularity for community members. WARPs and CERTs should not consider themselves to be in competition. Both models can work together to share workload and both have strengths to specialise in particular areas. The WARP model *augments* the CERT model. WARPs can be viewed as a way of making CERT citizen outreach more effective.

Workshop Six

Co-chairs

WARPs and BS7799

Natasha Stonestreet, Jim Sunderland

See workshop notes

Feedback session: The forum agreed that WARPs can provide important support in BS7799 compliance. Information security awareness and education is becoming increasingly important, particularly as the way that information is held and managed is rapidly changing.

WARPs act as ‘virtual security gurus’ in providing a clear process for responding to a security incident and this supports BS7799 compliance. Whilst senior management does not always understand what a WARP is and how it works it can be successfully demonstrated that WARPs will assist with compliance and therefore are worth investment. WARPs were described as being ‘virtual security gurus’.

Workshop Seven

Co-chairs

Education and health sector

David Harley, Malcolm McKeating

See workshop notes

Feedback session: The WARP model is viable across the education and health sector whether in hospitals, schools, trusts or partnerships. Evidence of benefits and timely reporting is important in such regulated environments. ‘Managed growth’ of these WARPs is also an important consideration. It is important that WARPs do not become too bureaucratic and therefore ineffective.

Workshop Eight

Co-chairs

WARPs and e-crime/police

Mick Humphrey, Martin Wright

See workshop notes

Feedback session: Organisations should be aware of the increasing risk of being sued if client data is stolen from their systems. WARPs should be promoted as a way of preventing this.

The forum also considered the possibility of developing ‘junior WARPs’ to provide IT security for university and school student computers. It was also suggested that these WARPs could be managed by IT or business students.

The forum also discussed that e-crime issues should now become a standard part of community crime prevention lectures and tours.

Insurance of physical assets requires that certain measures are in place. In the future this may also be the case for 'cyber insurance' and WARPs could play an important role in this.

Workshop Nine **Partnerships for WARP development**

Co-chairs Peter Daniel, Peter Kendal
See workshop notes

Feedback session: This discussion focussed on the sustainability of the WARP programme. It considered ways to develop new WARP communities particularly when their success relies on trust and willingness to share information. It was recognised that this can be difficult in new communities.

The forum suggested that feedback, case studies, reports on benefits and actual cost savings are all important to ensure both management buy-in and community development.

It was suggested that a paper should be written for the WARP toolbox which provides guidance on ways to make a WARP community as effective as possible.

Workshop Ten **Business benefits of WARPs**

Co-chairs Bruno Brunskill, Diane Howorth
See workshop notes

Feedback session: The business benefits of a WARP include:

- filtered information;
- sharing verified information;
- sharing and solving problems in a forum environment;
- reducing duplication of effort;
- meeting Gershon efficiencies; and
- reducing costs – SMEs spend an average of £843 resolving each virus

Businesses can be persuaded of the value of WARPs by quantifying savings. This could include presenting a case of how much money they could lose if they DON'T have a WARP. This includes financial and man hour losses. It was suggested that businesses could 'guest' on existing WARPs in order to understand the tangible benefits. This was agreed providing 'guests' do not have access to confidential information.

Findings and recommendations

The findings and recommendations session was led by Alan Paller. He commented on how successful the event had been and stated that the only remaining question for the day was 'why aren't there at least FIFTY WARPs?'

He emphasised the benefits of the WARP model that had come out during the forum. This included the concept of sharing verifiable information. The model ensures that all information shared can be relied upon to be useful and accurate as it is based on the direct experience of the trusted community.

WARPs should aim for the co-operation levels currently experienced by CERTs. CERTs have developed strong communication links both nationally and internationally. WARPs should look to this model to develop WARP-to-WARP communication, particularly where similar software is used.

Alan suggested that WARPs should now look for ways to promote WARPs more widely. For examples WARPs may consider offering articles on WARP successes to local newspapers, specialist press and local authority and education newsletters to help reach new target audiences.

Final conclusions and close

Judy closed the forum with some thoughts on the day. In particular she emphasised that WARPs are for the *community*. They should be developed as the community finds useful. NISCC offers help wherever necessary but recognises that WARPs will branch out and become whatever they need to be. Judy encouraged attendees to spread the WARP message.

She thanked attendees for their participation and their valuable work championing WARPs. She also thanked Alan Paller for his important involvement in both the programme and the forum event and thanked Peter and his team for his continued work on the WARP programme. She hoped to see all attendees at the WARP Forum 2007.



NB - Over 90% of delegates agreed that the forum had been successful and that they would attend a follow up event. For a more detailed analysis see [Feedback](#).

Workshop feedback notes

Workshop One

WARPs and e-Government

The workshop consisted of existing WARP practitioners and people seriously considering starting one mainly from the public sector. There was consensus that WARPs are a cheap and effective way of increasing public bodies' quality of information and increasing the prospects for effective sharing.

A number of drivers were identified that provide the rationale for developing WARPs to support e-government initiatives:

- a. ODPM 'take-up' campaign
- b. CPA BCP & Security Audit
- c. Efficiency agenda
- d. Benefits of sharing expertise and resources
- e. Better knowledge
- f. Planned re-structuring

Much of the conversation was about building communities or partnerships. WARP communities are not often congruent with other sharing communities and it will not always be useful to follow the patterns or partnerships set by e-Government relationships. A number of alternative approaches were considered:

- a. start small with the 'willing'; this was thought to be the most promising way to generate a WARP community;
- b. business driven communities are also a promising route to explore;
- c. mandate communities, but coercion seldom provides an enduring basis for new public sector business;
- d. use existing communities but with care because not all will be suitable;
- e. supplier driven.
- f. Engagement is the most important element
- g. Plug into the needs of Senior management
- h. Inform and enlist enthusiasts to get the ball rolling.

Workshop Two

Resilience building with WARPs

- Insurance -
Policy OR core business???
- Educate and inform
- Knowledge is power (no power – nothing)
- What do you do when it happens? TRUST
- SHARED: Risk
Cost
Complexity

Lessons learned in a shared community

ISO 27001

- BCP
- IA
- Risk Management
- Incident Response
- Good Corporate Governance
- Protecting
- Reputation

CC Act 2005

- Forensics
- Supply Chain issues
- Data classification – trends
- Plan –v-Respond
- People – make it happen
- Filtering information, knowing what you know!
- Shared Services – Efficiency
- Think National/Regional – act Local
- Adding Value

Workshop Three

WARPS in central government

The following key points were raised in discussion by and considered by those people attending the group to require addressing in the near future:

- A Warning Advice and Reporting Point (WARP) is a trusted community, which acts as the outreach component for the Computer Security Incident Response

Team (CSIRT). The WARP is required to promote trust relationships and improve interaction and to facilitate the work of UNIRAS.

- Protocols and information exchange requirements for interaction between the WARP and the CSIRT are currently not in place and are a prime requirement. Whereas the CSIRT has a mission and scope, the WARP does not and there is a need for a Service Level Agreement between the two. IERs should address any filter mechanisms requirement between the WARP and the CSIRT, together with the requirements for mandatory reporting.
- A key requirement for the WARP is management buy-in. In order to gain it, there would need to be Key Performance Indicators and metrics for measurement of effectiveness.
- A key requirement for Government WARPS is that information is considered to be 'need to know' - however this needs to be defined.
- There is a requirement for the articulation of the definition and service level agreements for incident response between the Managed Service Provider and the Client, in part to articulate business impact of an incident.

Workshop Four

WARPs for SMEs

99% of British businesses are in the SME sector, and historically have co-operated little, competed a lot, and tended to trade in a localised, limited and familiar market place.

On-line activities give SMEs access to the global marketplace. They also work the other way, giving the world-wide community of thieves, cheats, con-artists and trouble causers global access to SMEs.

Underpinning the workshop was the view that the SME response HAS to be improved security, and that WARP services are a key piece of the information security jigsaw.

The workshop was well attended, and quite lively discussion raised many questions, but few answers. After a brief summary of the services which a WARP offers, the main items discussed were –

How to educate the SME sector about the fact that they do have a problem – information security – to sort out, before setting out to help them solve it, whether by using a WARP or by some other method.

How to make the existence of an SME WARP known to the target sector.
Suggestions here included using existing agencies and their established channels of communication – Business Link, Chambers of Commerce, Trade Associations, etc. – and making as much use as possible of local news media

How to define logically related communities within the very wide SME category – geographical? Employee numbers? Industrial Classification? Turnover?

How to establish, in a highly competitive sector, the value of ‘Trusted Sharing’, of the availability of un-biased, or at least transparent, advice and help for mutual benefit.

The place of Information Security product and service vendors in the scheme of things, and their role in raising awareness (for whatever motives)

The concept of WARP membership as one step in the process of engaging in Information Assurance/Security

The value of homing in on one area of current concern – such as VoIP – as a focus of interest to attract members/subscribers

The value of the act of joining a WARP being a positive and deliberate step for an SME to take, a conscious move towards Information Security, as opposed to just automatically having membership of a free service

The need for SMEs to realise that the large influential organisations in the marketplace are moving more and more into electronically conducted supply chains, and that information security in some quantifiable form is a necessary pre-condition to an SME becoming – or remaining – part of those supply chains.

In summary, the message was that SMEs don't HAVE to take information security seriously – survival of their business is not compulsory.

Workshop Five

International Developments & CERT cooperation

Workshop participants discussed various motivators and forms of cooperation with CERTs and among WARPs themselves. Following was concluded.

Cooperation between the small but growing WARP operator community is taking already taking place. Common goals are some of the more obvious motivators here and the quarterly WARP Operator Forum brings peers together for jointly tackling cooperation issues.

While cooperation between CERTs and WARPs is still to be proven in field, hopefully benefits can be seen from both sides. Participants agreed that if WARP and CERT models are applied properly and strengths of one are overlapped with the other's weaknesses while working together, both models, and more importantly, their constituencies could benefit. WARPs may be weaker at technical know-how to solve all issues but their more flexible and less formal nature helps to get a better overview of what concerns its community members really have. CERTs at the same time are

highly technical but sometimes more distant from their constituencies. So long UNIRAS is the only CERT officially involved with UK WARPs but this topic has potential for growth as WARPs become more prevalent.

There is interest in the WARP model from outside UK and maybe some non-UK WARPs maybe even come around in 2006. At the session, Swiss and Lithuanian representatives were participating and both of the co-chairs also added to the international mix.

Below are the notes and bullet points we made with Don for the session sum up:

Some parallels with CERTs:

Trust building and creating lines of communication (i.e. TF-CSIRT)

How to find the right contacts (RIPE IRT field)

WARP model is good in **getting people or organizations involved**.

There is **trust and contacts being built** at a local level.

1) WARP to WARP cooperation is growing and getting better.

For Filtered Warning service there are initiatives to share work load between WARPs and initiatives to have WARPs specialize in specific technical areas for the benefit of other WARPs

2) CERTs and WARPs are definitely not in competition.

3) WARP model is a more flexible and less formal model that augments CERTs in its reach and purpose

4) WARPs need a friendly CERT!

WARPs clearly should seek cooperation with CERTs as WARPs are in close touch with local communities and **know their concerns** in a way that CERTs simply could not.

WARPs don't necessarily have the **technical know-how** to find the solution themselves. Working with a **CERT could provide that**.

5) WARPs could prove to be useful for CERTs

For CERTs knowing that the solution they provided to the WARP request should be more fulfilling as they know that it really has an impact.

6) International and other cooperation developments:

We had Swiss and Lithuanian representatives present, High tech crime units / police is interested in WARP model. Hopes are high.

Workshop Six

WARPs and BS7799

The aim of the workshop was to show attendees how being a member of a WARP can help with compliance to the information security standard BS7799 through meeting the criteria of the following controls.

•Information Security Infrastructure A.4.1

The ability to select relevant platforms specific to your organisation and more so specific individual departments, helps information security coordination amongst larger organizations, encouraging the development of an internal security forum. The nature of the WARP ensures that members maintain contact with law enforcement authorities, regulatory bodies and information service providers. Contact with other WARP through the WARP bulletin boards will provide WARP members with essential advice.

•Reporting Information Security Events and Weaknesses A.13.1

The filtered warning service ensures events are promptly reported through the appropriate channels. The reporting of any observed or suspected security weaknesses in, or threats to, systems and services will be facilitated by the trusted sharing service of the WARP, as will the ability quantify and monitor incidents for learning.

•Management of Information Security Incidents and Improvements A.13.2 & Protection against Malicious and Mobile Code A.10.4

The ability to categorise the level of the filtered warning will ensure a quick, effective and orderly response to security incidents and assist with audit trails and logs. The warning service will also help the organisation to comply with detection and prevention controls, to protect against malicious software and to maintain appropriate user awareness.

•Security Awareness education during Employment A.8.2

The WARP will ensure all users are aware of the information security threats and concerns, which will also be supplemented by providing access to news, best practice advice and in Kent's case security awareness guidance.

Workshop Seven

Education and Health Sector

The Education and Health sectors in the UK have many similarities. Both are large communities comprising many more-or-less autonomous and very diverse (in size and function) sites linked by a common network. Both are of enormous concern on a personal and global level: security breaches in these sectors can have enormous impact on nearly all of us. Both have too large and diverse a user constituency to rely exclusively on a single WARP, but have enormous potential for bolstering self-help mechanisms with WARP networks. It isn't surprising, then, that it proved illuminating to consider both environments in a single workshop.

The session began with a presentation by the Co-Chairs, both currently employed by NHS Connecting for Health, on *WARPs and The NHS*. David Harley summarized the activities of the Threat Assessment Centre, which he managed until March, 2006:

- The Threat Assessment Centre was a mixture of a CERT (in that it drew upon specialized in-house expertise) and a WARP (only one full-time member, co-opting colleagues when appropriate and sharing administrative and incident management support with other teams).

- As well as supplying advice and consultancy, it acted as a triage point, redirecting enquiries outside its remit to the appropriate quarter.
- An advisory mechanism was maintained that took two main approaches: blog-like urgent alerts that sometimes prioritized prompt notification over exhaustive validation, if necessary, and longer-term briefings that were fewer and had a longer shelf life. These included FAQs and technical briefings. Use of a wide variety of information sources with variable reliability necessitated informed filtering and editing of relevant material.
- Prioritization of incident management over incident recording encouraged reporting.
- Current security concerns within NHS Connecting for Health centre on national application security: NHS sites cannot be reliant on advice and control from the centre, but need to foster self-reliance and participation in community resources.

•
Malcolm McKeating, manager of the Information Governance Security Team, expanded on the changing model, with direct support pushed to the NHS ceasing and support and helpdesk functions migrated from the centre.

- New IG discussion forums will provide an interactive medium for NHS staff to discuss issues and solutions with the IG security team, a focused Core WARP community, and other members, encouraging the sharing of information with peers as well as with the centre.
- FWAS software will be used to deliver best practice, alerts and incident information linked to relevant forum topics.
- The Core WARP community will react to incident reports and issues raised, and new best practice guidelines will be made available on the IG web site and via FWAS software.
- Guidelines will be provided and updated in response to input from the wider community.
- General forums will be open to the whole NHS, with specific areas restricted to the Core WARP group.

Andrew Cormack, Head of Security at UKERNA (United Kingdom Education and Research Networking Association) then offered a presentation from his experience on the academic/educational side that illustrated many similarities between the educational and health environments. Both consist of large communities distributed between disparate types and sizes of semi-autonomous institution using common networks (N3 for the NHS, JANET for the educational community). The academic community is served by JANET CERT, which is much larger than the Threat Assessment Centre, but serves a much larger constituency – also, NHS sites have always been encouraged to make full use of UNIRAS/NISCC advisories and resources.

- JANET CERT generally passes on advisories rather than originating them, but incorporates “the JANET experience” of the issues they deal with (e.g. specific threats, problems with new patches).
- Sites tend not to engage actively with CERT: they subscribe, but don’t invest.
- WARP members, on the other hand, are generally volunteers and by definition are engaged with the community.
- Many schools (like many smaller NHS sites) have no professional IT staff: they may not read advisories, and may not be able to make use of them if they do.

- A WARP can address organizational issues, not just technical issues.
- Some sites are already running WARPs or CERTs, or services that are functionally very similar, but aren't aware of it.

In the following discussion, in which input on how the NHS WARP strategy can work best was particularly requested, the following additional points were made.

- Internal incident management ties in with Codes of Connection and similar policy-related documents, as a means of encouraging good security practices
- The implementation of a WARP should mitigate problems with compromised sites before the disconnection stage is reached.
- NHS Connecting for Health is not resourced to take responsibility for security across the whole NHS.
- WARP economies of scale may be better than that of a CERT/CSIRT: apart from the reduced implementation cost of volunteer labour, a CERT may get many reports, generating a heavier workload than fewer reports to a WARP. A team of volunteers may do a better job than an overstretched individual or team of specialists.
- There is an instinctive feeling that there is a hierarchical, federated solution. One of the ways in which the model adds value is by being shared, and therefore cost-effective.
- Other value-adds: access to CERT-sourced information; discussion forum for sharing problems and solutions; access to proven expertise at and beyond centre.
- Successful implementation of a well-targeted, first sub-WARP will encourage formation of others. An infrastructure may be established by soliciting buy-in from end sites: a "trusting community" finds commonality of purpose and interest; a top/central body such as the core WARP community envisaged for the NHS may eventually become primarily focused on media relations.
- Different sites interface with different interest groups, leading to wider dissemination of information as trust networks evolve. Commercial agencies may benefit from sponsoring a WARP, for instance where it relates to a service they are providing.
- Expectation management is vital: expectations must not exceed what it's practical to deliver, and not everything can be mandated.
- There is a perception that security in schools needs to focus on paedophilia, but there are other important areas: general security awareness, good security practice, wider internet safety practice.

Workshop Eight

WARPs and e-Crime / Police

1) The workshop was well attended and by a wide variety of representatives. There was broad understanding of the complimentary approaches between WARPs and e-crime prevention, for example mechanisms for reporting and information sharing within a trusted environment.

2) A representative from Serious Organised Crime Agency (SOCA) highlighted the current issues regard theft of databases and thereafter individual's identity. He further spoke about the impact and activities of serious and organised criminal groups within

the field of electronic crime. An explanation was given as to the work currently being undertaken to create the National e-Crime Prevention Centre in Wolverhampton.

3) A discussion was held as to the level of knowledge by small / medium sized companies and voluntary and community groups of the risks from electronic crime. There was some early evidence to suggest that companies that fail to adequately secure their IT systems and in so doing cause loss or damage to another company are being held liable and legal actions are resulting. It is expected this trend may increase.

4) The workgroup discussed the method by which reports of electronic crime could be made to the police. It was emphasised that the usual means should be used, for example attending the local police station. The group discussed the potential reluctance of some companies to disclose losses from electronic crime attack. The representative from SOCA spoke about the agreed steps that will be taken with companies to secure and preserve evidence and reduce or prevent reputational damage.

5) A further discussion was held around the nature of preventative measures that should be used to prevent abuses of publicly available computers, for example those in libraries or community centres. In these regards WARP alerts or advisories can be quite specific and assist organisations facing similar risks to take preventative actions that meet precise needs. It was suggested that young people often have knowledge of successful preventative measures and a discussion should be held to consider the potential of there being a Junior WARP?

6) The situation within schools was discussed particularly where there are limited numbers of IT staff. WARPs for education could support such staff and again provide targeted advice and assistance. It was noted that BECTA supported this initiative:
<http://www.becta.org.uk/>

7) The workgroup discussed the opportunity of there being resources and training made available to existing and future police crime reduction officers so that they could offer some support to organisations on the risks they face and the measures they could take to prevent electronic crime. This was broadly welcomed.

8) Finally, it was recognised that within the framework of an anonymised and trusted environment reports of e-crime victimisation can be confidentially shared and highlighted to relevant agencies very quickly.

Workshop Nine

Partnerships for WARP development

The workshop was only attended by a few delegates, and because of this was able to focus on the specific partnership issues of the attendees. It was agreed that different partners would be required at different stages of the WARP lifecycle such as building the WARP, where hardware, software and communications service providers could be approached and organisations representing potential WARP users, such as SOCITM for Local Authorities, could be a partner to promote the WARP to the potential WARP community. The main partnership was seen as the WARP user community, and this was recognised as important for the sustainability.

It was suggested that the WARP community would benefit from utilising existing communities of interest as well as by establishing new groups. This would require spreading the key WARP messages and developing the trusted base to support information sharing. Discussions took place on:

- a. the type of user communities
- b. how to build those communities
- c. the complexity of establishing relationships (a people issue) to develop trust within the community.

The issues around building this partnership could be considered through responding to the following questions:

- a. Which organisations are potential members of the WARP community
- b. What do these organisations know or what are their perceptions about the WARP
- c. What are the key WARP messages that need to be communicated
- d. How and to whom at what level are these messages communicated within the organisation

Sustainability was recognised as a major issue for the WARP. Newly established WARPs should seek to create evidence based examples for dissemination, which could involve case studies and cost savings.

This could be a new section, as part of the lifecycle, within the WARP toolbox.

Workshop Ten

Business benefits of WARPs

1. The workshop consisted of people from all sectors keen to develop WARPs but who felt that preparing a business case would be particularly challenging.
2. Diane Howorth gave a valuable short presentation about business benefits to open the discussion. This concentrated on the two main themes of making the management of information risks more effective at the same time as using resources more effectively. Her main points were:
 - i. Sharing information reduces the risk of information systems being compromised and therefore reduces the corporate risk to organisations
 - j. WARPs enable organisations to limit the damage of unplanned events – both to the ‘bottom line’ and reputation
 - k. Efficiency savings are available through WARPs through reductions in overall manpower and other resources;
 - l. Membership of a WARP contributes to organisations’ Corporate Social Responsibility
 - m. WARP provides some building blocks to ISO/IEC 27001

3. It was agreed that WARPs provide an effective tool for information security management because they provide valuable outputs on all the issues that concern business and system managers. The outputs address the major concerns of most organisations namely:
 - a. what are the threats and how imminent are they? (WARP warnings)
 - b. how does the organisation identify its systems' weaknesses? (WARP warnings and notifications)
 - c. how can organisations avoid each learning the same lessons some of which are damaging? (WARP reporting)
 - d. where can an organisation obtain reliable infosec advice? (WARP advice)
4. The workshop also discussed cost issues. It is not always easy for a WARP business case to cope with the tension between the requirement for not-for-profit provision and the business need to show positive returns. Part of the challenge for the business case is to ascribe value to the features Diane listed, see paragraph 2.

Feedback

Specific Speaker Feedback

Grading	5	4	3	2	1	not answered
Introduction & Aims of the Forum – Judy Baker	23	22	11	1	1	2
Latest Developments Update – Peter Burnett	29	24	5	0	0	2
WARP Prospects – Alan Paller Director SANS	45	10	2	1	0	2

Workshop 1

Grading	5	4	3	2	1	not answered
WARPs & e-government – Bruno Brunskill & Judy Revell	0	8	1	0	0	0
Comments	Very informative. Noted that there is still confusion about the role of WARPs among people in the e-government. Lack of communication amongst local government an issue. Identification of 'who' should identify those bodies who should share information and at what level.					

Workshop 2

Grading	5	4	3	2	1	not answered
Resilience-building with WARPs – Mick Humphrey and Mark Brett	3	8	2	0	0	0
Comments	Good additional business benefits. Leaders needed to talk less and facilitate more. Some useful ideas. Presentation could have been livelier.					

Workshop 3

Grading	5	4	3	2	1	not answered
WARPs in Central Government – Ian Dowdeswell and Andrew Powell	3	6	1	0	0	0
Comments	Good but session would have benefited by more Q&A time. Too short! v good well led!					

Workshop 4

Grading	5	4	3	2	1	not answered
WARPs for SMEs – Geoff Smith and Jim Sunderland	5	6	2	0	0	0
Comments	Reinforced the scope of WARP could be tailored for 'local' use. Full of good ideas, insight and general information in the key issues. Needed to be better facilitated & more structure.					

Workshop 5

Grading	5	4	3	2	1	not answered
International developments and CERT co-operation – Don Stikvoort and Mehis Hakkaja	2	3	5	0	0	0
Comments	Waiting to see the development & collaboration of this BT CERT/WARP model. I missed having more WARP operators joining the session. Maybe next year. Involve real CERT team to discuss.					

Workshop 6

Grading	5	4	3	2	1	not answered
WARPs and BS7799 – Natasha Stonestreet and Jim Sunderland	2	1	2	3	1	0
Comments	I ran the workshop. Not quite enough participation, but good level of interest. Natasha was good. The other speaker was doing most of the talking. No objectives were defined for this session. Excellent. There was more of an emphasis on the BS7799 standard rather than how WARP compliments the best practice. Useful contacts made. Too much lecturing on 7799. Not enough time for Natasha's WARP input. Useful but presentation could have been more engaging and more WARPs oriented.					

Workshop 7

Grading	5	4	3	2	1	not answered
Education and Health Sector – Malcom McKeating and David Harley	2	5	2	0	0	0
Comments	Excellent from a comms perspective; how do we address these 2 sectors and what key messages do we need? Good synergy between H&E could lead to improved relations in future. Poor start but strong finish! Good to discuss how large organisations can implement a WARP (or groups of WARPs).					

Workshop 8

Grading	5	4	3	2	1	not answered
WARPs and e-crime/police – Mick Humphrey and Martin Wright	7	7	6	0	1	2
Comments	Supportive ideas generated for future development. A stronger focus on specifics of WARPs as discussion tended to expand WARPs too far and more consideration to business requirements/information exchanges. This topic was very interesting and threw up lots of issues. The biggest challenge may be the ability to bring a prosecution across international boundaries. Could have discussed threats more but some very good peripheral info – not as targeted to business requirements. Very useful needs a lot of funding!! A very good approach about the usefulness of using WARPs to inform about e-crime. Leaders needed to talk less & facilitate more.					

Workshop 9

Grading	5	4	3	2	1	not answered
Partnerships for WARP development – Peter Daniel and Peter Kendal	2	0	2	0	1	0
Comments	Group too small to share experience. Good discussion but low turn-up. Mostly those who wanted to hear from the community turned up.					

Workshop 10

Grading	5	4	3	2	1	not answered
Business Benefits of WARPs – Bruno Brunskill and Diane Howorth	2	2	2	0	0	0
Comments	The business objectives were diversified. Useful ideas for business case and food for thought. Well done Bruno & Diane!					

General Workshop Feedback

Grading	5	4	3	2	1	not answered
	12	23	13	1	0	11
Comments	Interesting. Great idea! Sums up the day and helps to finalise your thoughts. Great idea to have open workshops rather than presentations. Need to cut down the total number. Less topics, higher quality. Unfortunate technology did not work but presenters gave good account. Plenty to think about. Fantastic. So much learning from this session. Feedback plenaries are rarely productive, and this was no exception.					

What other workshop topics you would like to see in the future.

Working with software suppliers.
 To provide development and management assistance for future WARPs by the existing ones.
 Probably enough topics but more WARP operator experience/interest sharing.
 Use of virtual/electronic forums for international WARPs.
 Case study including resources cost, implications, efficiency savings.
 Best Ways to implement WARP strategies.
 Promoting and sustaining WARP membership.
 Evolution of WARPs toward further services/models.
 Legal/Liability issues related to WARPs
 Setting up a WARP - overview.
 Working with NCC & IAAC to see how they can help WARPs.
 Incident response methodology.
 WARP FWA defaults.
 Sharing intelligence on attack modes.
 Internal threats.
 Strategies for forensics.
 Knowledge management essentials.
 Engaging community and keeping them involved.
 Information sources.

Trust and expectations.
 Implementing and structuring WARPs in large organisations.
 Expansion of working WARPs, more examples.
 How to start a WARP – what does it look like?
 Management engagement
 Effect monitoring
 Psychology of cooperation and why some people will not participate despite the benefits.
 War stories, examples of WARPs that exist today.
 Hardware & software deployed in existing WARPs

What was the most useful part/session of the day?

Alan Paller	12 people nominated Alan Paller as the most useful	vision and enthusiasm; an interesting and entertaining speaker, could have listened for longer. presentation provided interest, humour encouragement to all who listened. very good – informative deeply committed and knowledgeable. Exceptionally good speaker.
Networking	12 people nominated Networking as the most useful	Informal contact. Opportunity to exchange ideas.
Workshops	7 people nominated Workshops as the most useful	Facilitated debate, brought about issues and perspective and gave grounds to improve what may be and what should be. Always a good way to encourage more detailed discussion about pros and cons. Would have liked to attend more than two. International developments & CERT co-operation. E-crime. WARPs in central government. Resilience-building with WARPs
Feedback Sessions	4 people nominated feedback sessions as the most useful	Especially the one on International developments & CERT co-operation.
General	Each had benefit. All sessions useful, some more entertaining than others. Meeting with people running or planning other WARPs and sharing experiences. Meeting all the WARP people. The whole day was effective, useful and interesting. WARP prospects. Plenary.	

What was the least useful part of the day?

WARPs and e-crime session. (x2)
 Workshop advertising!
 Lunch – too long. 45 mins would have sufficed.
 Coffee break.
 Some workshops won't work without sufficient numbers.
 Late finish – got to get back to Midlands.
 Wish I could have attended all workshops.
 Nothing.
 Feedback session.
 No particular one.

All sessions useful. (x2)
 Not sure there were any parts that were not beneficial.
 BS7799 workshop.
 Resilience-building with WARPs workshop because it did not seem to cover its title topic.
 Introduction.
 There was no session that I felt was time-wasting.

Was anything you expected to hear about not mentioned?

“Typical” hardware/software used in existing WARPS eg proprietary, open source.
 Promoting WARPs.
 Relationships with NCC, IAAC etc and how that could help with the running of WARPs.
 Insider threat.
 The importance of education for our target communities. You cannot raise awareness when discussing with people who know little of the subject.
 Where does WARP start/stop and a CERT begin?
 Not a lot being said about what WARPs could do, on a technical level, and exploration of trust and what it means and how to create it etc.
 Session giving practical demo of existing WARP and users. Surprised that not included in any presentation. Future of WARPs – possibilities not explored sufficiently.
 FWA functionality.
 Relationship of WARPs to other security initiatives.
 Feedback from operational WARPs.
 Case history from concept to implementation, especially the detail of how the software was being used.
 Structures and workings of WARPs.
 I thing a ‘real WARPs’ presentation would be good at an event like this – 3 WARPs – 5 minutes each showing exactly what their members get for each service.

Would you attend a similar event next year?

<p>Yes</p>	<p>52</p>	<p>Would like to see some case histories, practical implementations. On-going interest. Good networking, good touch with the community. Good chance to network and for moral support. Useful discussion forum and networking opportunity. Very useful, good discussions. I knew about WARPs before I came here but didn't really understand how powerful they can be. More experience of operational WARPs. Keeps your mind sharp/good networking. I want to be a champion for the WARP cause! Need to keep up-to-date with progress. It's an excellent way to keep abreast and know who you are really dealing with – talking to a real person face to face makes a big difference. Useful as a WARP operator. The informal style of the day put people at ease and subsequently made the workshops relaxed and productive. Awareness of developments. Networking with others towards same aims. To keep up with developments. Networking/information sharing. Even if I am not involved in WARPs next year I will attend if Alan Paller is a speaker! Interesting to see where it all goes. The sales pitches for the workshops were a welcome novelty, and entertaining too. The emphasis that the critical component for WARPs is a sense of humour? Very good for the exchange of information. Because at the moment WARPs are what I spend most my working day on, and I am committed! To keep up to date with useful developments, to keep abreast of ideas and general networking.</p>
<p>No</p>	<p>2</p>	<p>But it is clear from one feedback form that this person did not have a good understanding of WARPs. The final comment was, 'do more for those who are trying to find out about WARPs'. No, if I felt it impacted on my role as DSO.</p>

Part Four – Administration and Facilities

Grading	Excellent	Very Good	Fair	Poor	No answered
Advance notice and information	31	23		1	5
Reception process & helpfulness of the organizing team.	43	14	0	0	3
Forum documentation pack	6	22	9	0	3
Venue facilities	38	20	0	0	2
Food and beverages	31	25	2	0	2
Any additional comments on administrative arrangements	<p>From Chris Davis Dept Transport, Thanks to supporting role staff – their humor, friendly and informative approach made event a success (as well as content). Very professionally organized. Could do with more soft drinks and fruit after lunch. Central, covered size, quality good – excellent choice. Very good.</p>				

Overall effectiveness of the day

Grading	5	4	3	2	1	not answered
	21	34	3	1	0	1
Comments	<p>Shorter workshop sessions. Networking was most productive part of the day. Highly successful – excellent interaction and valuable information exchange. Well conceived. Liked the format. Enjoyed the networking. International and e-crime were very useful. It gave scope information, food for thought and networking/contacts. Very good summing up and thought provoking ideas. Networking opportunities particularly appreciated. As also the update on how WARPs were developing. Very good interaction</p>					

Other Comments

Good to hear from afar.

Too many consultants were at the event and not enough end-users/organisations.

Do more for those who are trying to find out about WARPs.

3 min intros to workshops were entertaining, but the time could possibly have been saved by typing the material up and distributing in advance.

A real WARPs presentation

Longer and broader campaign to foster attendance.

It would be interesting to hear more about vendor viewpoints – I understand sensitivity that creates.

Found the day to be very useful.

More opportunities to attend workshop. Formal session on management.

Would have liked to have attended more workshops – reduce session time and lunch.

The venue was superb and should be used again.

Extremely well organised.

Organise workshops of similar content but short enough to allow attendance to more than one.

Report from actual WARPs.

Perhaps a brief summary of each workshop sent by e-mail to participants after the event.

Another confirming e-mail nearer the time of the event may have been welcome. I think the first confirmation I received was about eight weeks ago, a great event anyway.

Reduce the number of workshops. I would have liked to attend more than those I did. Perhaps video recording workshops and handing out a DVD later and giving workshop handouts.

Please keep the format and humour. The pace and session lengths are just about right. Shorter lunch perhaps. Well done Peter and all the team! (from Chris Davis Department of Transport).