



“Expanding the WARP mission”

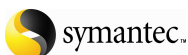
The 4th Annual WARP Forum 2008

The 4th Annual WARP Forum took place on Tuesday 3rd June 2008 at the Law Society building in the heart of London.



The event was attended by over 100 delegates and included attendees from Holland, Ireland and Canada with presentations from the US, Italy and Greece. As usual, the Annual WARP Forum offered delegates a unique opportunity to listen to presentations from experts in the field, network with other people active in the area, and to share advice and experiences. For some delegates it was also the first opportunity to learn about WARPS and gave them a chance to talk to people who had had experience of setting up and running WARPs.

This year the event was generously sponsored by the 7 organisations shown below.



Timetable

The timetable for the day was as follows:

09:30	<u>Welcome</u>	Desmond Hudson CEO Law society
09:40	<u>Opening keynote</u>	Director CPNI
10:00	<u>WARP developments and case studies</u>	
	<u>In praise of WARPs</u>	Bruce Thompson London Borough of Hillingdon
	<u>WARP Operator's Forum</u>	Tony Proctor University of Wolverhampton
	<u>WARP Trust development and aspiration</u>	John Harrison WARP Programme
	<u>WARP Managed Service Platform</u>	Alan Garwood WARP Programme
10.50	<u>The Law Society WARP – why and how?</u>	Timothy Hill Law Society Andrew Rose Clifford Chance
11.10	<u>WARPs in Europe, an ARECI perspective</u>	Karl Rauscher Bell Labs Fellow
11.40	<u>How WARPs might have helped in Athens 2004</u>	Alexis Iliadis Director, Telecoms and Electronics 2004 Olympic games
12.00	Round table discussion	Chairs introducing their workshops
	1 Physical security	Ian Horseman-Sewell
	2 Personnel security	Campbell Murray
	3 Incident management and forensics	Neil Hare-Brown
	4 Legal and regulatory compliance	Neil Lovell
	5 Trends and changes in electronic security	Paul Wood
	6 Information sharing across systems	Andrea Rigoni

14.00 Workshops

Workshop 1A

Chair

Physical Security

CPNI

Workshop 1B

Chair

Personnel Security

Campbell Murray

Workshop 1C

Chair

Incident Management and Forensics

Neil Hare-Brown

Workshop 1D

Chair

Trends and Changes in Electronic Security

Paul Wood

15.00

Workshop 2A

Chair

Physical Security

CPNI

Workshop 2B

Chair

Personnel Security

Campbell Murray

Workshop 2C

Chair

Legal and Regulatory Compliance

Neil Lovell

Workshop 2D

Chair

Information Sharing across Systems

Andrea Rigoni

16.00 Forum Feedback

Peter Burnett and chairs

16.30 Summary and closing remarks

16:45 Close of Forum

09.30

Welcome address

The forum was opened by Desmond Hudson, CEO of the Law Society.

Desmond welcomed everybody to this year's forum and started by describing the security needs of his 100,000 plus members. He highlighted the move to e-conveyancing, on-line Legal Aid and e-document management. He described how important the WARP model was in helping to deliver the necessary security to protect the reputation of the legal profession and, what is, a valuable national asset (estimated at 2% UK GDP).

He thanked CPNI for their support and encouraged other professional Bodies to consider the WARP approach.

[Back to timetable](#)

09.40

Opening keynote



The opening keynote speech was provided by the Director of CPNI. His presentation concentrated on the integration of physical, personnel and electronic security and other future development with respect to WARPs

Main points

- Establishment of WARP Trust increases independence of WARP programme
- Establishment of WARP MSP will help to overcome financial and practical hurdles;
- Integrated, holistic approach to security is to be encouraged but cannot be imposed. Experts should stay within their individual fields but must be more familiar with others' and able to cooperate with each other more.

Director CPNI concluded by referring to his now famous "Cyber terrorism is a myth" statement, and put this into context. The threat of physical attack is still much higher than the threat of cyber attack but the latter is still a real and significant threat. This must be recognised so we don't concentrate on one to the detriment of the other.

[Back to timetable](#)

10.00

WARP Development and case studies

In praise of WARPs



Bruce Thomson is from the London Borough of Hillingdon and is currently their IT Security Manager.

Bruce described his experiences since taking on the role in 1999 and went on to talk about information sharing and the importance of building trust.

Main points:

- Information sharing WARPs aren't complex. They are easy to setup with the help of the WARP Toolbox.
- The Managed Service Platform looks very promising for the future.
- The benefits of setting up a WARP are tangible and real.
- WARPs for 2012. Absolutely crucial – please support this in any way you can.

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides1.ppt>

[Back to timetable](#)

The WARP Operator's Forum



Tony Proctor is the principal consultant and WARP manager at University of Wolverhampton, presently supporting the WMC and EMG WARPs

Tony is currently chair of the WARP Operators' Forum and gave a description of its function, its current state and its future plans .

Main points:

- Perceived inertia on part of central government
Policy on e-security unclear
Lack of funding
- Several high profile security incidents have produced increased interest in WARPs
- WOF e-forum is functioning
- WOF is strong, democratic and diverse with a loud voice

Tony concluded with a worrying quote from an NHS IT Manager in the Midlands:
“Security is just not a priority at the moment!!”

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%202.ppt>

[Back to timetable](#)

WARP Trust Development and Aspirations



John Harrison has been working with CPNI as a consultant with the WARP programme since its inception and is now involved with taking the programme forward.

John gave an update on the state of the WARP Trust and described his hopes for the future.

Main points:

- Governance of WARP programme to move to the WARPs themselves (WOF)
- Sustainability needs critical mass
- Focus on key sectors with a multiplier
- WARP MSP will drive down costs for WARPs and create revenue to cover the costs of the WARP programme.

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%203.ppt>

[Back to timetable](#)

WARP Managed Service Platform



Alan Garwood is a software development consultant who has been working on the WARP Programme for many years. He described the development of the a WARP Managed Service Platform and the benefits of using it to implement WARP services

Main points:

- For an annual fee the WARP Managed Service Platform offers the following;
 - All required hardware, software, hosting and commonly required content
 - Automatic backup and patching
 - Secure access
 - Site can be customised to the specific WARP using colours, logos and fonts
 - Shared document repository

Alan concluded by stressing that the MSP offered a cost effective solution to provision of a WARP whilst simultaneously supporting the WARP programme.

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%204.ppt>

[Back to timetable](#)

10.50

The Law Society – why and how?



Timothy Hill is the IT Programme manager for The Law Society.

Andrew Rose is a specialist in IT Security at Clifford Chance, one of the world's leading law firms.

Main points:

- Deregulation means more corporate ownership of, and IT investment in, the legal profession.
- With advent of e-conveyancing, electronic data storage and communication, and online access to legal aid, the legal profession must become very conscious of the need for electronic security.
- There are over 100,000 solicitors nationally who need to become aware of IT security
- WARPs offer a feasible way to reach this huge community starting with a City of London WARP.
- Initial take up of the trial has been disappointing. In future must create more reasons for members to “visit” and use active promotion.

Andrew Rose said that valuable lessons had been learnt from the WARP trial and that the recommendation is that it should proceed. Some of the lessons learnt from the trial were that it was difficult to engage as participants were too busy and they already had existing ways of sharing information. Andrew quoted a solution to this identified by Matthew Smith with the IsfL LCWARP:

“Face to face sharing is straightforward, although it can take some time to develop into trusted sharing. Sharing using electronic means on the face of it would seem to be just as straightforward which is why it was quite surprising when it took some time to get off the ground. It is now working very effectively and is in use everyday by our WARP members who know they will get a valuable response from their peers, sometimes within minutes. The breakthrough came for us when we set the default on the system for members to receive everything, and they then had to elect not to receive information. This enabled them to see the value in real time sharing and also of being in control.”

Plans for the future include:

- Initiate a ‘real’ WARP (beyond the trial)
- Expand membership
- Try to create “reasons to visit” the WARP
- Use our expertise and experience to support the Society in promoting other legal WARPs

In conclusion Andrew described the concept of a circle of trust and said that expanding this in a controlled way was the key to taking WARPs forward.

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%205.ppt>

[Back to timetable](#)

11.10

WARP in Europe, an ARECI perspective



Karl Rauscher is a Bell Labs Fellow and Executive Director of Bell Labs Network Reliability and Security Office

Karl described the findings of an EU programme entitled The Study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI). In particular he described Recommendation 4 of the study which had implications for the WARP Programme.

Main points:

- Recommendation 4 (supported by 86% of the stakeholders involved in the study) states that member states and private sector should establish formal means of information sharing to improve the restoration of infrastructure ...throughout Europe.
- WARPs are an excellent next step for European stakeholders because
 - they already exist
 - they are flexible
 - they can provide both mesh and star architectures
 - they can grow with their community
 - they can share within sectors, across sectors, inside and outside national boundaries

Conclusion:

- Information sharing within and among critical infrastructures is vital to public safety.
- The WARP approach is a world class role model that many can learn from.
- The WARP model has the flexibility to accommodate the special needs of Europe.

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%206.ppt>

[Back to timetable](#)

11.20

Coffee break (networking)



11.40 How WARPs might have helped in Athens 2004



Alexis Iliadis was the Director of Telecommunications and Electronics For the 2004 Olympic Games.

He described the huge task of setting up the massive electronic infrastructure necessary for a 17 day event.

Main points:

- Plan early for a huge event like this
- Due to the temporary nature of the event, a lot of infrastructure is exposed and installed outdoors or in temporary buildings, posing a potential physical security weakness.
- Local communities and local security forces must be involved at the earliest opportunity.
- Building one team spirit and common culture including sponsors, subcontractors and authorities are essential elements for success.

Alexis concluded by saying that WARPs would have been a very useful in helping achieve all the above. Close working relationship with the local communities is essential and that's where WARPs can be of great value in the upcoming LONDON 2012 Summer Olympic Games

[Slides](#)

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%207.ppt>

[Back to timetable](#)

12.0 Round table

The six workshop Chairs introduced their workshops. Slides are available for each presentation/workshop as well as the Chairman's introduction.

Chairman's Introduction

CPNI

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W1a.ppt>

1 Physical security

Ian Horseman-Sewell

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W1b.ppt>

2 Personnel security

Campbell Murray

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W2.ppt>

3 Incident management and forensics

Neil Hare-Brown

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W3.ppt>

4 Legal and regulatory compliance

Neil Lovell

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W4.ppt>

5 Trends and changes in electronic security

Paul Wood

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W5.ppt>

6 Information sharing across systems

Andrea Rigoni

Slides

<http://www.warp.gov.uk/Index/Forum/Presentations2008/Slides%20W6.ppt>

13.00 Lunch (more networking)



Delegates networking over an excellent lunch

14.00 Workshop sessions

Each workshop covered one of six areas each of which addressed an area into which WARPs could expand. Delegates could attend two workshops of their choice during the afternoon sessions. The findings of both sessions were later fed back to the forum

in the final session of the day. Chairs were asked to provide comment on what they considered to be the most important issues to come out of the workshops. A summary of the issues covered is included in the workshop reports below with the principle conclusions summarised in the "[Report back](#)" section.

Aims of each workshop:

To debate the topic under consideration in a structured way and to reach a consensus on recommendations for the WARP programme to take forward.

Workshops 1A and 2A Physical Security

Chairs: CPNI and Ian Horseman-Sewell, G4S Security

Discussion:

The two sessions were approached in a similar way with each considering the following:

What physical security information should be shared under Warnings, Advice and Reporting?

The feeling expressed in session 1 was that the number of alerts and warnings in the physical security domain would be very small compared with those already being received in the electronic security area. This could create a "dilution" problem. The area where content could be made immediately available would be best practice and advice. Problem was, would IT managers use it?

What are the issues/barriers to sharing this type of information?

Both sessions agreed that the principle barrier to expanding WARP coverage would be the perception of the users (particularly IT managers). People thought that many WARP operators and users do not currently see physical security as relevant to their needs. Changing this attitude was seen as a key issue and how to do this was discussed at some length.

What are the benefits in sharing this information?

The principle benefit was perceived as raising awareness of a holistic approach to security and thus achieving greater effectiveness. The ability of communities to respond to criminal activities would be enhanced.

How could this sharing be done within/between WARPs?

One train of thought was that it was no good providing information if users don't perceive a need for it. Some people suggested separate mechanisms, similar to WARPs for those interested in physical security. But it was pointed out that that would be the opposite of a holistic approach. The counter argument to this was that if it is not there for use when it IS needed there will never be a migration to a more holistic approach. Chicken and egg!

[Conclusions](#): see report back

[Back to timetable](#)

Workshops 1B and 2B Personnel Security

Chairs: Campbell Murray, Encryption and CPNI

Discussion:

The first workshop acknowledged that despite a renewed sense of thinking as regards IT security within organisations, it was still relatively easy to obtain company and employee information since staff are the weakest link and prone to responding to phishing emails. The workshop chair emphasized how much easier it was to send a simple phishing email than one with a malware.

How can WARPs add value here? It was suggested that WARPs could only act as a resource - they cannot be adapted fully in this area of security because one is dealing with human nature and a sense of endless curiosity.

The second workshop re-emphasised the fact that personnel security in the public sector presents its own challenges. CPNI already has a number of guidance measure available such as: Threats, Challenges and Measures to increase personnel security, pre-employment screening and risk assessment but all of these only go as far as being pre-employment checks. Once the new staff member enters the organisation, a whole host of issues could influence the employee to be 'devious' and create security vulnerabilities. Future guidance measures suggested were: Ongoing personnel security, security culture, overseas checks and off shoring.

[Conclusions](#): see Report Back

[Back to timetable](#)

Workshop 1C Incident Management and Forensics

Chair: Neil Hare-Brown, QCC

Discussion:

The session started with a presentation overview of incident management and forensics which set the scene for discussion which revealed the following:

What Incident management/forensic information could be shared under Warnings, Advice and Reporting?

The synergy between incident management and 'Reporting' was clear but most discussion focussed on the need for clear standards and categories to enable the efficient sharing of information and the aggregation of data for use as metrics. QCC outlined a number of standards addressing for example: Definition of Incident Types, Definition of Impact. This was considered important to enable quality business decisions to be made on where and how much to invest in preventative measures. It was commented that few organisations gather this type of incident data which is a lost opportunity.

What are the issues/barriers to sharing this type of information?

The lack of common standards was seen as a major barrier with one WARP operator saying that they had just started to look at standards for Incident Types within their WARP Community. Ian Bryant reported that he had been working on a Cabinet Office report which made recommendations on these standards and when it is published it

could be made available to the WARP communities. One WARP operator said they would like to adopt this standard rather than reinventing the wheel.

What are the benefits in sharing this information?

The principle benefit of standard incident reporting types/impact was to enable the aggregation of data across the WARP community to provide useful metrics. It was also suggested that if all WARPs adopt the same standard this aggregation of data could be much wider. It was suggested that the National Audit Office would be very interested in these statistics for government related communities such as Local Authorities.

How could this sharing be done within/between WARPs?

The need for standards for sharing information on incident management and forensic information could be done through a set of standard categories adopted by all WARPs in their reporting templates. In particular the WARP Managed Service Platform could be upgraded to include these categories 'out of the box' for all new WARPs. Commercial companies could also be encouraged to adopt the same standard to enable the wider aggregation of data.

[Conclusions](#): see Report Back

[Back to timetable](#)

Workshop 1D Trends and Changes in Electronic Security

Chair:

Paul Wood, Messagelabs

Discussion:

Security in virtual worlds - a WARP in Second Life?

Whilst social networking sites have been seen as issues in acceptable use policies for attendees of the workshop, there were no consistent views as to the best way of handling access. Some commented that controlling the use of such sites in the workplace would not stop people using them at home. For most the main danger was seen as people giving away personal information that could prove useful in identity theft or spear phishing or whaling attacks - the key WARP function being providing advice on how to safely use such sites, and how to recognise dangerous use of harvested information. A WARP in "Second Life" was seen as somewhat difficult, given anonymity and lack of trust - all you could really do is provide advice, but why would anyone take it? It was noted that such tools are used for business purposes now, for example to provide training areas.

Analysing emerging threats

It was suggested that WARPs could use their specific knowledge of the communities that they serve in order to analyse emerging threats to see if they are relevant. The WARP could be used as a method of providing management information to its members based on raw information reported in. The possibility of receiving useful management information back from the WARP would encourage reporting - closing the feedback loop.

WARPs working with the local community

There was a question from the floor regarding how a WARP could provide advice to a local community on specific security and privacy issues. A discussion followed that

suggested maybe members of established WARPs could spread their influence to local areas of the community they touch - for example, WARP members may want to provide advice to the schools their children attend. Helping in the community will reduce exposure to risk - the more people become aware of IT security issues, the less likely they are to become victims of e-crime.

[Conclusions](#): see Report Back

[Back to timetable](#)

Workshops 2C Legal and Regulatory Compliance

Chair: Neil Lovell, Securecoms

Discussion:

The session started with a short presentation to stimulate discussion which revealed the following:

What Legal and Regulatory compliance information could be shared under Warnings, Advice and Reporting?

Many organisations have compliance teams and some work closely with their security teams. It was suggested a very useful thing to share was anything to do with the interpretation of compliance relating to security as this was often difficult to judge. This would add most value if done in the same sector and/or the same compliance area e.g. Local Government, DPA or PCI.

What are the issues/barriers to sharing this type of information?

Not all compliance teams work closely with security teams so sharing good practice in this area would also add value. Sometimes it is not clear what legal or regulatory compliance is relevant to an organisation which makes it difficult to engage with others.

What are the benefits in sharing this information?

Sharing good practice security for compliance which is benchmarked with your peers would ensure that investment in security is set at a level which is not too high or too low. If WARPs started to share compliance related information then it may be possible to get endorsement for WARPs from legal and regulatory bodies such as the Information Commissioners Office. These bodies could then use WARPs as an information distribution channel.

How could this sharing be done within/between WARPs?

Categories on compliance could be created in the WARP FWA and WARP MSP to facilitate information sharing. To address the Compliance/Security team benefits a special interest group could be setup, either meeting face to face or via the WOF on-line discussion forum. This would be open to Security and Compliance teams to encourage a dialogue and agreement on interpretation of good practice.

[Conclusions](#): see Report Back

[Back to timetable](#)

Workshops 2D Information Sharing across Systems

Chair:

Andrea Rigoni, Symantec

Discussion:

Following a presentation by Andrea to provoke thoughts, the following discussion points were raised:

Language Issues

It was noted that any systems sharing between nations will always encounter language issues. It may be necessary to agree a common language for sharing, with translation for local distribution. This is in effect what is happening now between some organisations. The problem with this method can be the potential for inaccuracies in translations, possibly changing the meaning of the information shared.

Competition issues

Sharing can be influenced by sector - some sectors may be able to share without any problems regarding competition, one example of this was power companies across Europe, in other sectors competition between organisations may provide problems. CNI organisations have a role in encouraging sharing.

Integration of new sources

Some comments were made regarding commercial sources, one of which featured in Andrea's presentation, regarding the costs. It was noted that the costs of such services tend not to be "WARP Friendly".

Technical vs. process issues

It was noted that there are some real technical issues regarding sharing information between systems - for example finding a common format that two systems can "understand", but there are also process issues. Solving technical issues may not achieve information sharing if the process issues are not also examined. The limited sharing between systems already occurring between CSIRTUK and WARPs still requires processes to be in place to provide context information and confirm the severity based upon community.

[Conclusions](#): see Report Back

[Back to timetable](#)

16.00 Report back on workshop topics

Each workshop chair delivered the conclusions of their respective workshops.

Workshops 1A and 2A Physical Security

- The consensus of opinion in the first session was a definite "maybe". It was seen as a good thing but people felt that currently most WARP users would not perceive a need for physical security.
- Consensus was that we should start to introduce physical security information on the WARPs and in parallel raise awareness among IT managers and other users as to its relevance for them.

- The second session felt that expansion of the WARP coverage was essential and would appeal to the commercial/private sectors so being a valuable asset in achieving critical mass.
- A trial was suggested with an existing WARP and the Olympic WARP seen as a possible “shot in the arm” where the integration of physical security and electronic security would have obvious benefits

[Back to timetable](#)

Workshops 2A and 2B Personnel Security

- The current WARPs offering could be expanded to include staff training such as Security Awareness Training;
- Include Cascade Line Training Management where staff would benefit from more frequent training and where Line Managers could keep closer tabs on their staff;
- For WARPs to work in this area of security, it would be vital to create a framework in order to correctly monitor and evaluate the nature of each incident.
- One of the ways in which personnel security vulnerabilities can be inhibited is to set up an HR WARP, which would in turn, communicate with the IT WARP creating a safer and vulnerability-free zone. However, this could also create a silo effect, with either WARP ending up not speaking to one another and preventing a free flow of information;
- Alternatively, in the absence of an HR WARP, the IT WARP could create quality training material for HR so as to involve HR more on a day-to-day basis rather than just exist as the organisation’s hire-and-fire officers;
- Or WARPs, in its current form, can send out email alerts to HR which in turn are sent to the staff. WARP advisory emails should only act as a guideline and not as a rigid textbook of commands with the risk of creating an interdependency on information and losing the context of the issues at large.

[Back to timetable](#)

Workshop 1C Incident Management and Forensics

- The main recommendation is that the WARP programme should adopt the proposed standard from the Cabinet Office proposal when it becomes available. The WARP MSP should be updated to include these categories in its reporting template and the same categories should be included in the standard FWA categories to support incident warnings and advisories.

[Back to timetable](#)

Workshop 1D Trends and Changes in Electronic Security

The conclusions of this workshop session were that the WARP programme should:

- Not setup WARPs in virtual worlds, but look to provide sector specific advice on their use;
- Exploit opportunities to develop a layer of management information on reported information to help decide if a particular threat is relevant to a community;
- Seek to support local communities where WARP members have influence to extend security knowledge for the common good.

[Back to timetable](#)

Workshops 2C Legal and Regulatory Compliance

The main recommendations are:

- Sharing information on interpretation would add real value and save costs
- Sharing experiences between combined security/compliance teams should be encouraged by creating a special interest group
- The WARP FWA and WARP MSP should include categories to aid sharing information on legal and regulatory compliance
- The Information Commissioners Office should be asked to endorse WARPs and provide relevant content

[Back to timetable](#)

Workshop 2D Information Sharing across Systems

The conclusions of this workshop session were:

- For the WARPs, discounts would be required should commercial sources need to be integrated;
- There are technical and procedural issues regarding the sharing of information between systems - for example, shared information may need a local context to assess severity;
- Language can be a major barrier to international sharing;
- It is important to identify communities that either want to share, or have to share - otherwise competition issues could get in the way.

[Back to timetable](#)

16.30 Summary and closing remarks

Peter B closed the Forum the delegates for a very successful day and with an invitation to a final networking session over refreshments.

NB - 100% of delegates who completed the feedback questionnaire agreed that the forum had been successful and that they would attend a follow up event. For a more detailed analysis and for all comments see [Feedback](#).

[Back to timetable](#)

Feedback (45 respondents)

Your backgrounds

Who were you representing?

	Existing	Potential	Total
A WARP Operator	12.1%	17.2	29.3%
A WARP Provider	5.2%	5.2%	10.3%
A WARP Champion	13.8%	8.6	22.4%
A WARP Member	12.1	5.2%	17.2%
Totals	43.1%	36.2%	

Other	20.7%
Government Department representative Guest of a member NICC Provider of Business Resilience Services Transport for London CPNI (two attendees) Dutch delegate PCEU Vendor Gov Cert Netherlands Sponsor	

Your views on the Forum

Very useful	5	4	3	2	1	Not useful
	31.1%	55.6%	13.3%	0%	0%	

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

<ul style="list-style-type: none"> - Sessions from the users - WARP Development and Law Society WARP - European commission links - CEO opening speech - Workshops x10 - Practical sessions – MSP, Law Society WARP and Athens - Networking x2 - WARP development and case studies – workshops - Networking and session 2 on information sharing - MSP presentation - Examples of existing WARPs - Panel and workshops - Law Society WARP (three attendees said this)

- Olympics session x3
- WARPs in Europe x2
- Panel
- The morning presentations x3
- All useful
- Break out sessions
- Workshop on incident management

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

- Panel session
- Nothing
- Very high level conceptual sessions
- Round table discussion a little rushed
- Message labs session
- Olympics session
- WARPS in Europe
- All useful
- All of value x3
- Workshop attended; a lecture, not a workshop! (sales pitch)
- Round table discussion
- Workshops. too long. x2
- Whilst very useful, some workshop time could have been used to expand some of the morning topics
- Directors speech
- Wrap up session

Was anything you expected to hear about not mentioned?

- Not a lot of information on techniques for improving trust and uptake which seem to be the main problem areas
- No (x13)
- In my opinion we should talk more about failures and problems. The key note from the Law Society was very interesting because the speakers pointed out very precisely why it didn't work yet. That is the best way to discuss further improvements
- More mention of difficulties
- Acting on threats as opposed to threats
- FoI requests to WARP providers and operators
- International WARP progress
- Briefing on plans for information sources

Would you attend this event next year or recommend it to a colleague?

YES 100% NO 0

Comments:

- Gave overview of WARPS. Difficult to answer other questions as need to review suitability for our business.
- Nice lunch, thank you
- Enjoyed the guest speakers
- More time for discussion would have been useful in the Symantec session
- Would have liked greater explanation about what CPNI does and who can access their services if at all.
- Really well organised
- Trust was a theme that came out several times; worth a workshop next year?
- Olympic lectures interesting, perhaps more technical debrief on attacks and risks.
- A very informative and beneficial event
- The introduction to the workshops before lunch can, as far as I'm concerned be left out. I can make my choice based on written information.
- Not enough time for discussions between workshops and round table session
- A panel discussion would be interesting
- I notice the scope has broadened since my last visit 2 years ago
- Good networking

16.0 Expanding the role of WARPs

Given the discussions and information you have heard today, please give your opinion on the importance to you of expanding the role of WARPs in the following areas:

	Critical	Very important	Quite important	Not important
Physical security	9.3%	53.5%	34.9%	2.3%
Personnel security	20.0%	60.0%	20.0%	0%
Incident management & forensics	33.3%	40.0%	24.4%	2.2%
Legal & regulatory compliance	19.5%	43.9%	31.7%	4.9%
Trends/changes in electronic security	21.4%	59.5%	19.0%	0%
Information sharing across systems	35.7%	54.8%	7.1%	2.4%

“Weighted results” scores out of 100

Physical security	67.4
Personnel security	75.0
Incident management & forensics	76.1
Legal & regulatory compliance	69.5
Trends/changes in electronic security	75.6
Information sharing across systems	81.0

Comments:

- All critical for a holistic view of security may not be appropriate for all communities
- All are at least very important but other Fora/Networks may be better at sharing information
- WARPs must find a way to reach critical mass. One possible way is via added function
- Would like to have attended them all
- Losing the focus of WARP may dilute effectiveness so caution is recommended
- More chance to attend other sessions?
- I doubt if you should use one WARP for both IT and physical/personnel security. Are these the same people to work on security.
- WARP seems to work best as part of holistic information assurance philosophy

Potential WARP Operator only

Given what you have heard today:

Will you be supporting the creation of a WARP in your community?

YES **94.4%** NO **5.6%**

Will you use the managed service platform to provide WARP services?

YES **71.4%** NO **28.6%**

Comments:

- Need to evaluate whether we are likely to get sufficient critical mass and see if we can generate funding first.
- WARP model being proposed as part of Fraud Management Standard
- Not sure to both questions. Would like to discuss further with WARP members, users, etc.
- Possibly, if format fits needs etc, an issue for further consideration
- Undecided, not sure where TFL would sit. However an Olympics WARP would be considered.
- Caveat, the community is not cohesive so some work to do
- (won't be supporting/providing WARP services) "unless it will be implemented in the Netherlands
- WARP MSR – RoI difficult to justify on costs
- Don't know yet (re use of the managed service platform to provide WARP services).
- Looking at our own developments, a lot is similar to MSP (with exception to FWA)

Other comments

- Relating the WARP initiatives to other cyber security issue and activities, the bigger picture
- Role of education, training and skills. We're dealing with the world today, but this will change. How are we impacting the education and training of new grads, i) in the technology sector, ii) in the business sectors i.e. grads/post grads who will move into employment in technical roles. But, also where, for instance, is the connection between Law schools and Law Society so that new lawyers come into the profession not only aware but have expectation and experience and so for other professions/sectors.
- A very useful day and thoroughly enjoyable
- Message labs, emergent threats. Room format did not support a 'Round table' discussion (very well).
- Working for the MoD WARP, I found the forum extremely interesting. Unfortunately the MoD do not share IT information because of restrictions.

However, it was good to learn what happens in the Private Sector. Well done to those who organised this event.

- My compliments for the organisation. Very nice atmosphere, good food. Thanks for a nice congress
- Potentially useful for raising awareness of specific tools/ IT systems, etc, and how to use them. Main issue is difficulty in assessing level of coverage i.e. who has taken notice of the item raised.
- A really excellent day. I learnt a lot and meet many interesting people. Trust is key to an effective WARP. We have done a fair amount of work in this area and would be pleased to progress this if it would be useful next year. Also motivating operators/users to access WARP is a common problem amongst portal type providers. We have some thoughts on how this may be progressed. The Demos pamphlet on Business Resilience (2006) is good for holistic security.
- A useful and informative day. Thanks for the invitation, I will definitely seek to progress WARP membership.
- Very good day, thanks for putting it together
- Very well organised meeting. Good occasion to meet people and network. At end the energy (that was there during the day!) seems to have gone down a bit.

[Back to timetable](#)