

WARP member benefits statements

(V1.0) July 2005

Keywords

WARP, case study, benefit

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk>

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

Contents

1	Scope	2
2	Background	2
3	Definitions and abbreviations	2
3.1	Definitions	2
3.2	Abbreviations.....	2
4	Benefits statements	3
4.1	Implementing security policies (Ref: LCWARP/05/01).....	3
4.2	Security and outsourcing (Ref: LCWARP/05/02)	4
4.3	Spoofed email (Ref: LCWARP/05/03).....	5
4.4	Web defacement (Ref: LCWARP/05/04)	6
	History	7

1 Scope

This document describes the benefits derived by anonymised WARP members from the three WARP services, filtered warnings, advice brokering and trusted sharing. The case studies describe benefits in terms of cost savings, increased security and increased capability.

2 Background

The argument and business case for creating a WARP is enhanced significantly by real examples of benefits derived from existing WARPs and their members. To help capture these benefits, and to aid subsequent analysis, a benefits template has been created which ensures the information is in a consistent format. This template has been used in this document and also protects the identity of the WARP member. However, the source WARP is identified within a unique reference number for each benefits statement to help maintain the provenance and credibility of the information. This document will be updated regularly as new benefits are captured from WARPs and their members.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply:

Advice Brokering Service:	A service where members can learn from other members initiatives and experience.
Filtered Warnings Service:	A service where members receive only the security information relevant to their needs.
Trusted Sharing Service:	A service where reports are anonymised, so members can learn from each others attacks/incidents without fear of recriminations or embarrassment.
WARP:	Warning, Advice and Reporting Point - a unit or team providing the three basic services (Filtered Warnings, Advice Brokering, and Trusted Sharing) to a defined community, in accordance with the NISCC WARP model and approved variants.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

CERT:	Computer Emergency Response Team
FWA	Filtered Warning Application
NISCC:	National Infrastructure Security Co-ordination Centre

4 Benefits statements

4.1 Implementing security policies (Ref: LCWARP/05/01)

Author and/or source

Email from WARP member

WARP Service which facilitated the benefit:

Filtered Warnings		Trusted Sharing		Advice Brokering	✓
-------------------	--	-----------------	--	------------------	---

Description of WARP member’s environment:

LCWARP member representing one of the 33 London Boroughs with responsibilities for e-services.

The issue to which the benefit relates:

It is difficult to find free, practical and appropriate advice and support from others who share similar concerns in local government. For example, it takes time to develop information security policies and it is often difficult to know if one has covered all the issues appropriately.

Actions taken to resolve the issue:

Sharing copies of existing and draft policies with members of LCWARP help to clarify ideas and develop suitable and appropriate policies. In the case of a Wireless Access Policy sharing the draft copy with other members gave them a starting point in this area and provided me with a degree of confidence that I was on the right track.

Type(s) of benefit:

Cost saving	✓	Increased security	✓	Increased capability	✓
-------------	---	--------------------	---	----------------------	---

Description of benefit:

Information sharing has reduced the amount of time I needed to spend on the development of this particular policy significantly and has removed any need to call upon a consultant. I estimate the savings at £2k. The policy document resulting from the collaboration is in my opinion better than it would have been even had a consultant been employed. In this instance the benefit has been qualitative and put us in a better position to meet the future needs of the organisation.

4.2 Security and outsourcing (Ref: LCWARP/05/02)

Author and/or source

Email from WARP member

WARP Service which facilitated the benefit:

Filtered Warnings	✓	Trusted Sharing		Advice Brokering	
-------------------	---	-----------------	--	------------------	--

Description of WARP member’s environment:

LCWARP member representing one of the 33 London Boroughs with responsibilities for contracts and security.

The issue to which the benefit relates:

Service provision is outsourced in our case but clearly has to be managed. We need tools to help us perform the management task effectively and efficiently. This will ensure the availability of payroll and human resources services both for the Council and for a large number of schools in the area.

Actions taken to resolve the issue:

Subscription to the Filtered Warnings service.

Type(s) of benefit:

Cost saving		Increased security	✓	Increased capability	✓
-------------	--	--------------------	---	----------------------	---

Description of benefit:

The WARP service has been of particular benefit to us. The cost/time saved cannot be readily estimated but in terms of maintaining the availability of the service and the perception that goes with that it is clearly invaluable. We also consider using the provision of WARP advisory messages as an additional tool and means of measuring our BS7799 Compliance in relation to authorised changes of software packages. Thereby improving standards and managing the confidentiality, integrity and availability of our systems.

4.3 Spoofed email (Ref: LCWARP/05/03)

Author and/or source

Report from a WARP member

WARP Service which facilitated the benefit:

Filtered Warnings		Trusted Sharing	✓	Advice Brokering	✓
-------------------	--	-----------------	---	------------------	---

Description of WARP member’s environment:

LCWARP member representing one of the 33 London boroughs.

The issue to which the benefit relates:

The borough reported that they had received an email indicating that a particular email address within their organisation had been used to send infected emails. This naturally caused concern particularly when some detective work revealed that there was no evidence of these emails actually being sent.

Actions taken to resolve the issue:

The borough asked if the LCWARP could help and the LCWARP in turn sought the help of UNIRAS. UNIRAS were able to trace the problem and it turned out that the original infected email actually came from a private individual who probably did not even realize that his PC was infected with the Klez virus.

Type(s) of benefit:

Cost saving	✓	Increased security		Increased capability	
-------------	---	--------------------	--	----------------------	--

Description of benefit:

The benefit to the borough was twofold. On one hand they were able to confirm that there were no infections within their organisation and that they were not responsible for infecting anyone else. On the other hand, through the LCWARP, they were able to access a service which would otherwise cost them a certain amount of money, namely UNIRAS help to trace the originating IP address.
--

4.4 Web defacement (Ref: LCWARP/05/04)

Author and/or source

LCWARP and one of the London boroughs

WARP Service which facilitated the benefit:

Filtered Warnings		Trusted Sharing		Advice Brokering	✓
-------------------	--	-----------------	--	------------------	---

Description of WARP member’s environment:

LCWARP member representing one of the 33 London boroughs.

The issue to which the benefit relates:

The LCWARP proactively monitor gov.uk websites for defacement and during this routine monitoring, it was noticed that the education server of one of this member borough had been defaced. On speaking to the contact there, it turned out that they did not even realise that the defacement had taken place. The problem was resolved by the borough and everything was back to normal. However, the defacements did not stop. It soon became clear that whatever the vulnerability was that was being exploited, it had not been patched.

Actions taken to resolve the issue:

The LCWARP turned to help from UNIRAS who in turn contacted CESG. Between them, they discovered that the vulnerability that was being exploited was a known WebDav vulnerability and this was soon patched. As a result, the defacements ceased.

Type(s) of benefit:

Cost saving	✓	Increased security	✓	Increased capability	
-------------	---	--------------------	---	----------------------	--

Description of benefit:

Through the LCWARP, this borough was able to access UNIRAS and make use of the services supplied by CESG – a route that might not normally be open to them. As a result of this, they were able to plug a security hole in their education web server which potentially could have opened it up to malicious defacement. This was done at minimal cost.

History

Version	Date	Description
V1.0	July 2005	First issue