

Document type: Reference

Tick-list categories for the WARP Filtered Warnings Service

(V1.0) June 2004

Keywords

[WARP, Filtered Warning]

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	Definitions and abbreviations	2
2.1	Definitions	2
2.2	Abbreviations.....	2
3	Background	2
4	Requirement	3
4.1	The requirements from the WARP member viewpoint	3
4.2	The requirements from the WARP operations viewpoint.....	4
5	Tick-list characteristics	4
5.1	Vulnerabilities and fixes	5
5.2	Incidents and Threats	8
5.3	Good Practice.....	8
6	Conclusions	9
	Appendix A: Microsoft product based categories	10
	Appendix B: Sun software product categories	12
	Appendix C: Linux software product categories.....	15
	Appendix D: Cisco product based categories.....	16
	Appendix E: Apache software product categories	20
	Appendix F: HP software product categories.....	21
	Appendix G: Incident/threat categories	23
	Appendix H: Good practice categories.....	24
	History	25

1 Scope

One of the original 'value add' propositions for WARPs was to provide a Filtered Warnings Service to members. To implement this service a categorisation of the information types available had to be devised together with a mechanism which captured the filtering criteria for each member. The process defined can best be described as members completing an on-line tick-list.

This report addresses the categorisation used in the tick-list.

2 Definitions and abbreviations

2.1 Definitions

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

CERT: Computer Security Incident Response Team, based on the model developed by the Carnegie Mellon University.

Filtered Warning Service: Members will complete an on-line 'secure' tick-list which identifies their area of interest. Warnings and Advisories from a number of sources, including UNIRAS and the membership itself, will be filtered against the tick-list criteria for relevance and urgency and disseminated via email in a timely manner.

2.2 Abbreviations

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

GUI: Graphical User Interface

NISCC: National Infrastructure Security Co-ordination Centre

UNIRAS: Unified Incident Reporting and Alert Scheme

WARP: Warning, Advice and Reporting Point

3 Background

The UNIRAS team have considered the provision of a filtered Warning and Advisory service and have concluded, at least in the short term, that a detailed categorisation would be difficult and resource hungry to run operationally.

The provision of an automated service based on a 'list server' has therefore been investigated by the UNIRAS team who are considering using the following simple high level criteria:

- Alerts - Alerts eg malware warnings
- Advisories - Advisories covering topics as decided by the help desk
- Microsoft - Product Briefings
- Sun - Product Briefings
- Linux - Product Briefings
- Cisco - Product Briefings
- Apache - Product Briefings
- hpcompaq - Product Briefings

The UNIRAS argument for adopting this high level approach was that given they have such a large customer base, then managing the customer criteria would be resource intensive and so would the operational filtering process itself. Investing in the development of an automated capability beyond this high level approach is also considered difficult to justify. The details of how a customer selects their criteria had not been considered by the UNIRAS team.

By contrast, the WARPs will be relatively small communities who are looking for more value-add than that being proposed by the high level UNIRAS approach. It is argued that a more detailed tick-list criteria would provide this added value and given the smaller community would be easier to manage.

However, the operational task of implementing the filtering remains the same as for the UNIRAS team, but discussions with Microsoft indicated that they had the technology to semi-automate this process, and at no charge for the LCWARP.

4 Requirement

The requirements for the Filtered Warning Service can be considered from the users viewpoint (WARP members), and from the central operational WARP team who have to implement, manage and administer the service.

4.1 The requirements from the WARP member viewpoint

The tick-list must be:

- User friendly - simple and intuitive to fill-in;
- Efficient - taking an amount of time to complete commensurate with the value being provided;
- Relevant - must take into account the different interests and experience of the member by using appropriate language;
- Appropriate - ensuring that enough detail is captured to add real value to the filtering process;

- Compatible - with LCWARP member ICT systems – eg use standard browser technology and operating system;
- Maintainable - easy to check and keep up to date as their experience and interests change and mature;
- Safe - should also facilitate a ‘fail safe’ policy such that in the case of ambiguity or uncertainty, then source information will be passed on rather than being filtered out;
- Controllable - the ability to control the sources used in the filtering process.

4.2 The requirements from the WARP operations viewpoint

The tick-list must be:

- Simple to administer - and use in an operational environment such that it can easily be implemented on-line using good practice for usability;
- Maintainable – such that new categories can simply be added and old ones removed – this also extends to methods to help the user update their profile when the categories change;
- User friendly - it must be easy to use operationally when filtering information from a number of sources;
- Efficient – when used in a manual filtering process as well as in future automatic filtering systems by for example: reducing the risk of duplicate warnings from multiple sources or against multiple categories;
- Compatible - as far as possible, with interface standards, protocols and categories as they emerge from sources such as UNIRAS;
- Compliant - if any personal data is captured, the tick-list must comply with the Data Protection Act.
- Secure - by providing the member with the ability to indicate the sensitivity of the tick-list when completed, such that the appropriate safeguards can be implemented by the WARP.

5 Tick-list characteristics

It was originally thought that the problem of categorisation of Warnings and Advisories would have been solved by organisations such as CERTs, but this is still at an early stage of development and appears to focus on standards to enable the automatic sharing of incident/vulnerability information and analysis, using for example XML.

The categorisation for the WARP, it is argued, does not require such a rigorous approach, as manual intervention is accepted and indeed encouraged as part of the value-add process. Enquiries into categorisation frameworks, as required by the WARP, have so far failed to identify existing schemas which could be used.

However, it is believed that this problem is solvable, and has not been solved to date because the WARP concept is different to other sharing initiatives as it focuses on smaller communities. It is also felt that the operational problems of creating and managing the tick-list user profiles has also been a deterrent to creating this type of service, which is why this report also addresses solutions to this problem.

Consolidation of the feedback from early drafts of this report indicate there should be three top level categories:

- Vulnerabilities and fixes
- Incidents and Threats
- Good Practice

5.1 Vulnerabilities and fixes

Taking a steer from the UNIRAS approach, it can be seen that ‘products’ are a good focus for information on vulnerabilities and fixes, as it is argued the user will be more interested in a vulnerability/fix associated with a product they have purchased and installed than for example a security vulnerability associated with a network protocol.

Each of the following ‘product briefing’ categories have been investigated.

- Microsoft - Product Briefings
- Sun - Product Briefings
- Linux - Product Briefings
- Cisco - Product Briefings
- Apache - Product Briefings
- HP - Product Briefings

Microsoft

The Microsoft product support website at - <http://support.microsoft.com/default.aspx?scid=fh;en-gb;chooseproduct> was studied and the following five product categories identified:

- Office/Business Applications
- Windows Operating systems
- Home products
- Developer Products
- Server Products

The detail within each of these product categories is described in Appendix A, but it is interesting to note that Internet Explorer and Media Player, for example, are not listed. These bundled products will be included within the Windows Operating system category.

Security support for these 50+ products is provided via a single vendor site where users can register to receive alerts and briefings via email <http://www.microsoft.com/security> . There is no facility to filter from this site.

The Filtered Warning Service has been provided with these 5 first level categories, shown in **Bold** in Appendix A, and the associated second level categories, shown in **Bold Italic**.

Sun Microsystems

The Sun support site indicates the following high level software products:

- Operating Systems
- Systems and Network Management
- Server Products
- Application Development
- Desktop Products

Sun provide a software security information site at <http://www.sun.com/software/security>. Sun currently do not have an e-mail alert service for their security advisories, as they wish to allow customers to see an advisory “evolve” rather than send out a single alert when an issue has been fully researched and addressed as other vendors do. Current advisories can be viewed at http://sunsolve.Sun.COM/pub-cgi/search.pl?mode=results&so=date&coll=fsalert&zone_32=category:security .

The Filtered Warning Service has been provided with these 5 first level categories, shown in **Bold** in Appendix B, and the associated second level categories, shown in ***Bold Italic***. The third level categories are for information and could be used to help the WARP operator during the filtering process.

Linux

Linux is supplied by a number of organisations as distributions. Effectively a Linux distribution is a collection of OpenSource software (including the Linux Kernel itself) that has been bundled together into a coherent collection. Each distribution is made up of thousands of individual tools and programs. One of the values of using a branded distribution of Linux rather than downloading the source of every individual tool and compiling it yourself, is the availability of security information and patches. All the major Linux distributors provide security advisories, which you can subscribe to at the following URLs:

- Debian - <http://lists.debian.org/debian-security-announce/>
- Mandrake - <http://www.mandrakesecure.net/en/mlist.php>
- Redhat - <http://www.redhat.com/mailman/listinfo/redhat-watch-list>
- SuSE - <http://www.suse.com/en/business/maillinglists.html>

Due to the open source nature of Linux distributions the software collections are vast, and the bulk of the installed programs are of no interest to most users (they are small niche programs). No attempt has been made, at this stage, to break down the Linux section further than the distributions themselves. This can be addressed after gaining some experience of operating the service, some user feedback will be required to enable the provision of useful tick-list categories.

The Filtered Warning Service has been provided with these 4 first level categories, shown in **Bold** in Appendix C, and the associated second level categories, shown in ***Bold Italic***.

Cisco

Cisco provide a large number of hardware and software products, a detailed list of which can be obtained from <http://www.cisco.com/en/US/products/index.html> . In order to

prevent the top level of the Cisco tick-list from becoming too cluttered, the product list has been rationalised into the following high level categories:

- Switch/router/gateway Products
- Security and VPN Products
- Network Management Products
- Wireless Networking Products
- Content Networking Products
- IP Telephony

The Cisco security web site <http://www.cisco.com/security> gives access to all Cisco security initiatives, including the ability to view advisories and notifications. Advisories can also be received by e-mail, by going to http://www.cisco.com/warp/public/707/sec_incident_response.shtml#Subscribing and registering.

The Filtered Warning Service has been provided with these 6 first level categories, shown in **Bold** in Appendix D, and the associated second level categories, shown in **Bold Italic**. The third level categories are for information and could be used to help the WARP operator during the filtering process.

Apache

The Apache web server is included in all Open Source, and most Unix based, operating systems distributions and is also available separately on the Windows platform. Apache themselves do not distribute advisories by e-mail, but the vendor distributors do. Apache provide a weekly round up in their Apacheweek publication, which can be found at <http://www.apacheweek.com/>. The Apache Software Foundation provides more than just a HTTP server, and a number of other projects are in operation. In addition to the Apache projects, the extensibility of the Apache Web Server has lead to the availability of a large number of modules, some of which are large development projects in their own right. The Apache section will be split into Projects and Modules.

- Projects
- Modules

It should be noted however that most alerts will probably come from the Apache distributors (e.g. RedHat) rather than by subscribing to the Apache tick-list.

The Filtered Warning Service has been provided with these 2 first level categories, shown in **Bold** in Appendix E, and the associated second level categories, shown in **Bold Italic**.

HP

HP is an extremely diverse company, being made up of the operating divisions of both HP and Compaq, and with Compaq also including ex Digital and Tandem business units. In examining the available products for inclusion in the Tick-list, some of the older operating systems and related products have not been considered, but could be added if required. The operating systems not examined are: OpenVMS, MPE/iX and NonStop. The HP software products have been categorised into the following high level categories.

- Operating Systems
- Systems Management
- Networking

- Storage Products
- Application Development

Security support from <http://www.support.compaq.com/patches/mail-list.shtml> provides users with the facility to register to receive security alerts & email briefings.

The Filtered Warning Service has been provided with these 5 first level categories, shown in **Bold** in Appendix F, and the associated second level categories, shown in ***Bold Italic***. The third level categories are for information and could be used to help the WARP operator during the filtering process.

5.2 Incidents and Threats

The sources for this high level category will come from other LCWARP members via the Reporting and Trusted Sharing Service (RTSS), from NISCC, UNIRAS and other security organisations. The categories chosen include those from an analysis of the AusCert incident reporting form at <https://www.uscert.org.au/msubmit.html?it=3085>

- Target Groups
- Incident types
- Motive & effect
- Threat types

Details within these categories can be found in Appendix G.

The Filtered warning Service has been provided with these 4 first level categories, shown in **Bold** in Appendix G, and the associated second level categories, shown in ***Bold Italic***.

5.3 Good Practice

A product based approach for 'Good Practice' is not considered appropriate, partly because many good practice topics are vendor/product independent and indeed good practice should often be considered before the choice of product. Good practice advice associated with a particular product, outside the vulnerability/fix category, is not within the scope of the initial FWAS offering. However, feedback from the FWAS service will be used to judge demand for this type of service and it may be offered in the future.

It is therefore suggested that the topic based approach is more suitable, based on the three high level categories:

- Network security
- Application security
- Enterprise security

Details within these categories can be found in Appendix H.

The Filtered Warning Service has been provided with the 3 first level categories, shown in **Bold** in Appendix H, and the associated second level categories, shown in ***Bold Italic***.

6 Conclusions

This report takes a structured approach to look at the problem of creating tick-list categories for Filtering Warnings and Advisories. The solutions proposed are viable and will add real value to WARPs as well as to UNIRAS.

The key points are:

- A product based categorisation tick-list is recommended for the Vulnerability/fix high level category:
- Users would relate well to this approach as they use these products;
- Would be easy to populate, and involve the vendors participation;
- Filtering would be straightforward against this criteria;
- This approach could result in 500+ categorisation levels;
- An effective Graphical User Interface (GUI) for the tick-list implementation is vital to the success of a FWAS:
 - Makes the selection of 500+ categories feasible;
 - Would be used by both users and operational staff;
 - Makes the tick-list easy to maintain and keep up to date;
 - Dependent on GUI software development;
- Manual filtering against 500+ categories using the GUI is viable for typical WARP staffing levels but is dependent on:
 - An automated email system to manage distribution lists;
 - A clear understanding of the vendor product base;
 - The filtering process taking less than 10 min per item;
- NISCC/UNIRAS must have an ongoing role in the development of the FWAS to ensure that it is compatible with emerging standards and approaches, such as the XML based IODEF and VEDEF standards.

The creation of the tick-list categories was been a trivial task, caused mainly by the diversity of approaches used by different vendors. It is interesting to note that commercial security vendors who provide a filtering service provide filtering only at the product/version level, with no intermediate 'product type' categories. The approach described in this report is therefore seen as a real value-add for the FWAS. However, it also indicates that as this has never been done before, several iterations may be required to ensure the categories are fit-for-purpose.

Appendix A: Microsoft product based categories

1. Office/Business Applications

Access
Excel
Frontpage
2000
2000 Server extensions
2002
98 for Windows
for Macintosh
for Windows
Money
Office
Outlook
Powerpoint
Project
Publisher
Visio
Word
Works

2. Windows operating systems

2000
3.x
95
98
CEMillenium Edition
NT Workstation
XP
NT Server
Server 2003

3. Home Products

AutoRoute
Bookshelf
Encarta
Greetings
Home Publishing
MapPoint
Photdraw 2000
Picture It!
Plus!
Reference products
Games

4. Developer Products

DirectX SDK
Exchange
Visual
Basic
C
C++
FoxPro
J#
J++
SourceSafe
Studio

5. Server Products

BackOffice Server
Content Management Server
Exchange Servers
2000
5.5
Index Server
Internet Information Server 4.0
Internet Information Services 5.0
Mail Server
Mobile Information Server
Proxy Server
Sharepoint
Portal Server
Team Services
Small Business server
SNA server
SQL Server
Systems Management Server
Transaction Server

Appendix B: Sun software product categories

1. Operating Systems

Solaris

Sparc Edition

2.5.1

2.6

7

8

9

Intel Edition

2.5.1

2.6

7

8

9

Trusted Solaris

Sparc Edition

(versions)

Intel Edition

(versions)

Linux

See also RedHat And SuSE Linux categories

Sun Linux, 5.0

2. Systems and Network Management

Systems Management Tools

Solaris Bandwidth Manager

Solaris Resource Manager

Sun Management Centre

Sun Control Station

Solstice FTAM

Sun StorEdge OFS

VERITAS File System

Storage Management Tools

Solstice DiskSuite

VERITAS Volume Manager

VERITAS Storage Manager

Sun StorEdge Resource Management Suite

Sun StorEdge Utilization Suite

Sun StorEdge Performance Suite

Sun StorEdge Component Manager
Sun SAM-FS

Clustering/HA

Sun Cluster
Sun HPC Cluster Tools
Sun ONE Grid Engine
Netra High Availability Suite

Backup Tools

VERITAS NetBackup
Sun StorEdge Enterprise Backup
Sun StorEdge Instant Image
Sun StorEdge LibMON
Sun StorEdge Network Data Replicator
Sun StorEdge Availability Suite

Network Security

TCP Wrappers
SunScreen Firewall

Network Management

Solstice SunNET Manager
Solstice Cooperative Consoles
Solstice Enterprise Manager
Solstice Enterprise Agents
Sun Remote System Console

3. Server Products

Directory Servers

Sun ONE Directory Serer
Sun ONE Identity Server
Sun ONE Meta-Directory
Sun ONE Directory Proxy Server
Sun ONE Identity Synchronization for Windows
Solstice X.500 Directory

Web Servers

Sun ONE/iPlanet Web Server
Sun ONE Active Server Pages
Sun ONE/iPlanet Web Proxy Server
Sun ONE Portal Server
Apache

Application Servers

Sun ONE/iPlanet Application Server
Sun ONE Integration Server

Sun ONE Connector Builder
Sun ONE Message Queue

Messaging Servers

Sun ONE Messaging & Calendar Server
Sun ONE Instant Messaging and Solstice X.400 Messaging

4. Application Development

Development Tools

Sun ONE Studio
NetBeans IDE
Sun ONE Compiler Collection
Java SDK
 Standard Edition
 Enterprise Edition

5. Desktop Products

Thin Client

Sun Ray Appliance
Sun Ray Server Software

Desktop Applications

StarOffice
Netscape
Netscape Communicatio
Mozilla for the Solaris OE

Appendix C: Linux software product categories

Distributions

1. RedHat

6

7

8

9

2.1 Advanced Server

2. SuSE

Desktop Edition

Standard Server 8

Enterprise Server 8

3. Mandrake

7

8

9

9.2

Corporate Server 2.1

4. Debian

3.0

Appendix D: Cisco product based categories

1. Switch/router/gateway Products

Routers

SOHO
800 Series
1000 Series
1600 Series
1700 Series
2500 Series
2600 Series
3600 Series
3700 Series
7000 Series
10000 Series
12000 Series

Switches

Catalyst 2800 Series
Catalyst 2900 Series
Catalyst 3000 Series
Catalyst 3500 Series
Catalyst 3750 Series
Catalyst 4000 Series
Catalyst 6500 Series
Catalyst 8500 Series
Catalyst 8600 Series
LightStream
MicroHub 1538 Series

SAN Switches

MDS 9000 Series Multilayer Switches
SN 5400 Series Storage Routers

2. Security and VPN Products

Firewalls

PIX Series
Catalyst 6500 Firewall Services Module
IOS Firewall
Security Device Manager

Intrusion Detection/Prevention

Network IDS Sensors (Netranger)
Catalyst 6500 Intrusion Detection System Services Module
IDS Network Module for 2600, 3600 and 3700 routers

Host Intrusion Detection System (HIDS)
Cisco Security Agent

VPN Routers

Catalyst 6500 IPSec VPN Services Module
3000 Series VPN Concentrators
7000 Series VPN Routers
VPN Client

Access Control

Cisco Secure ACS

3. Network Management Products

VPN/Security Management Solution

Small Network Management Addition

Routed WAN Management Addition

LAN Management Solution

-or- a list of all the CiscoWorks modules:

CiscoWorks

Cisco Access Point Name Manager
Cisco Catalyst 6500 Series Network Analysis Module Software
Cisco Mobile Wireless Fault Mediator
nGenius Real Time Monitor
Cisco VPN Device Manager
CiscoWorks Access Control List Manager
CiscoWorks Auto Update Server Software
CiscoWorks Blue Internetwork Status Monitor Software
CiscoWorks Blue Maps
CiscoWorks Blue SNA View
CiscoWorks Campus Manager
CiscoWorks CiscoView
CiscoWorks Common Services Software
CiscoWorks Device Fault Manager
CiscoWorks Ethernet Subscriber Solution Engine
CiscoWorks Fault History
CiscoWorks for Mobile Wireless
CiscoWorks for Windows
CiscoWorks Gateway Statistics Utility
CiscoWorks Hosting Solution Engine
CiscoWorks Internetwork Performance Monitor
CiscoWorks IP Phone Help Desk Utility
CiscoWorks IP Phone Information Utility
CiscoWorks IP Telephony Environment Monitor
CiscoWorks IP Telephony Monitor
CiscoWorks LAN Management Solution

CiscoWorks Management Center for Cisco Security Agents
CiscoWorks Management Center for Firewalls
CiscoWorks Management Center for IDS Sensors
CiscoWorks Management Center for VPN Routers
CiscoWorks Monitoring Center for Security
CiscoWorks Network Connectivity Monitor
CiscoWorks QoS Policy Manager
CiscoWorks Resource Manager Essentials
CiscoWorks Routed WAN Management Solution
CiscoWorks Security Information Management Solution
CiscoWorks Small Network Management Solution
CiscoWorks Voice Health Monitor
CiscoWorks Voice Manager
CiscoWorks VPN Monitor
CiscoWorks VPN/Security Management Solution
CiscoWorks Wireless LAN Solution Engine

4. Wireless Networking Products

Aironet 1400 Series
Aironet 1200 Series
Aironet 1100 Series
Aironet 350 Series

5. Content Networking Products

7300 Series Content Engines
4600 Series Content Distribution manager
4400 Series Content Routers
500 Series Content Engines
CSS 11000 Series Content Services Switch
SCA 11000 Series Secure Content Accelerator
Distributed Director
Local Director
IP/TV 3400 Series Video Server

6. IP Telephony

IP Call gateways and Software

Cisco Billing and Measurements Server
Cisco CallManager
Cisco CallManager Attendant Console
Cisco CallManager Express
Cisco Conference Connection
Cisco Conferencing and Transcoding Feature for Voice Gateway
Routers
Cisco Emergency Responder
Cisco Gatekeeper External Interface
Cisco Gatekeeper/Multimedia Conference Manager
Cisco ICS 7750 Software

Cisco IP Manager Assistant
Cisco IP SoftPhone
Cisco Media Gateway Controller Software
Cisco MGCP IP Phone Software
Cisco Personal Assistant
Cisco SIP IP Phone 7960 Software
Cisco SIP Proxy Server
Cisco SRS Telephony
Cisco TCL Scripts for IOS Gateways
Cisco Unity
Cisco WebAttendant
Voice Interworking Service Module Software

IP Phones

7900 Series IP Phones

Appendix E: Apache software product categories

1. Projects

HTTP Server

Ant

APR

Avalon

Cocoon

Commons

DB

Incubator

Jakarta

James

Maven

Perl

PHP

TCL

Web Services

XML

Conferences

Foundation

2. Modules

(There are 262 different Modules. We will need feedback to put a good list in here)

mod_ssl

mod_perl

mod_tcl

mod_php

Appendix F: HP software product categories

1. Operating Systems

Tru64 Unix

HP-UX

2. Systems Management

Clustering

TruCluster for Tru64 Unix
Htpc ClusterPack for HP-UX

Server Management

Insight Manager
Remote Insight
Survey Utility
SmartStart

3. Networking

Network Management

HP Openview
ProCurve Network manager

ProCurve Switches

9300 Series

5300 Series

4100 Series

4000 Series

8000 Series

6108

2800

2600 Series

ProCurve Wireless Access Points

4. Storage Products

Storage management

OpenView Storage Area Manager
OpenView Storage Provisioner
OpenView Storage Management Appliance

Configuration Management Software

OpenView Storage Operations Manager
StorageWorks Command View XP
StorageWorks Command View EVA
StorageWorks Command View SDM (for VA)

StorageWorks Secure Manager XP
StorageWorks LUN Configuration Manager XP
StorageWorks LUN Configuration & Security Manager XP
Array Configuration Utility XE (for MSA)

Performance Management Software

OpenView Storage Volume Growth
StorageWorks Performance Advisor XP
StorageWorks Application Policy Manager XP
StorageWorks Auto LUN XP
StorageWorks Cache LUN XP
OpenView Storage Optimizer

Replication Software

OpenView Storage Mirroring
OpenView Continuous Access Storage Appliance
OpenView Storage Virtual Replicator
StorageWorks Business Copy XP
StorageWorks Business Copy EVA
StorageWorks Business Copy VA
StorageWorks Continuous Access EVA
StorageWorks Continuous Access XP and XP Extension

SAN software

StorageWorks Secure Path
StorageWorks Auto Path XP
StorageWorks Auto Path VA

Storage Array software

StorageWorks XP Disk Array Software
StorageWorks Enterprise Virtual Array Family Software
StorageWorks Virtual Array Family Software
StorageWorks Modular Storage Array 1000 Family Software
StorageWorks MA / EMA Family Software

5. Application Development

Java

Java 2 SDK for HP-UX on PA-RISC
Java 2 SDK for HP-UX on Itanium
Java 2 SDK for Tru64 Unix on Alpha

Compilers

Compilers and Tools for Tru64
Compilers and Tools for HP-UX

Appendix G: Incident/threat categories

1. Target Groups

LCWARP

UK

Worldwide

Public Sector

Private sector

2. Incident types

Electronic theft

Computer facilitated fraud

Unauthorised access

Website defacement

Interception

Virus, Worm, Trojan

Malicious probes/scans

Hoax or scams

Denial of Service

3. Motive & effect

Money/reward

Personal use

Competitor advantage

Disruption

Theft

Vandalism

Self aggrandisement

Indiscriminate

4. Threat types

Insider

External

Individual

Hackivism

Terrorism

Organised crime

Nation state

Appendix H: Good practice categories

1. Networks

Firewalls
Network component security
TCP/IP network product security
Virtual Private Networks (VPNs)
Wireless security
Intrusion detection
Network authentication
Client/Server security

2. Applications

Web application security
Email security
Anti-virus
Database security
Network management security
CRM
Desktop application security

3. Enterprise Security

Security architectures
Single sign-on
Public Key Infrastructure (PKI)
Smartcards
Web services security
Patch management
Software/system development security
Home-working
Business continuity
Information sharing
ISO 17799/BS7799
Data Protection Act
Security Policies
Security awareness/training
Acceptable Use Policy
Employee Internet Management
Handling eCrime

History

Version	Date	Description
V1.0	June 2004	First issue for WARP Toolbox