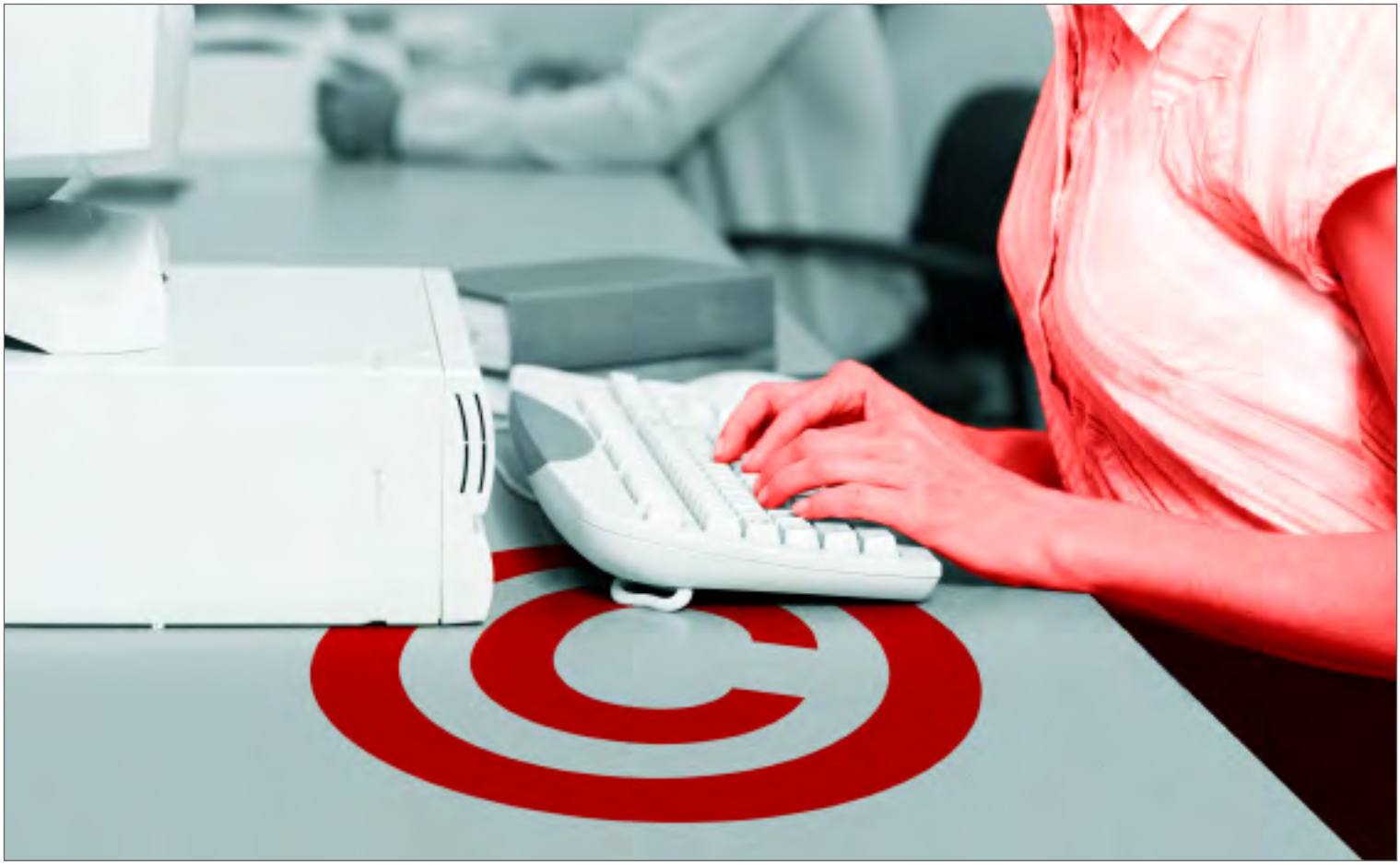


2005 COPYRIGHT AND SECURITY GUIDE FOR COMPANIES©

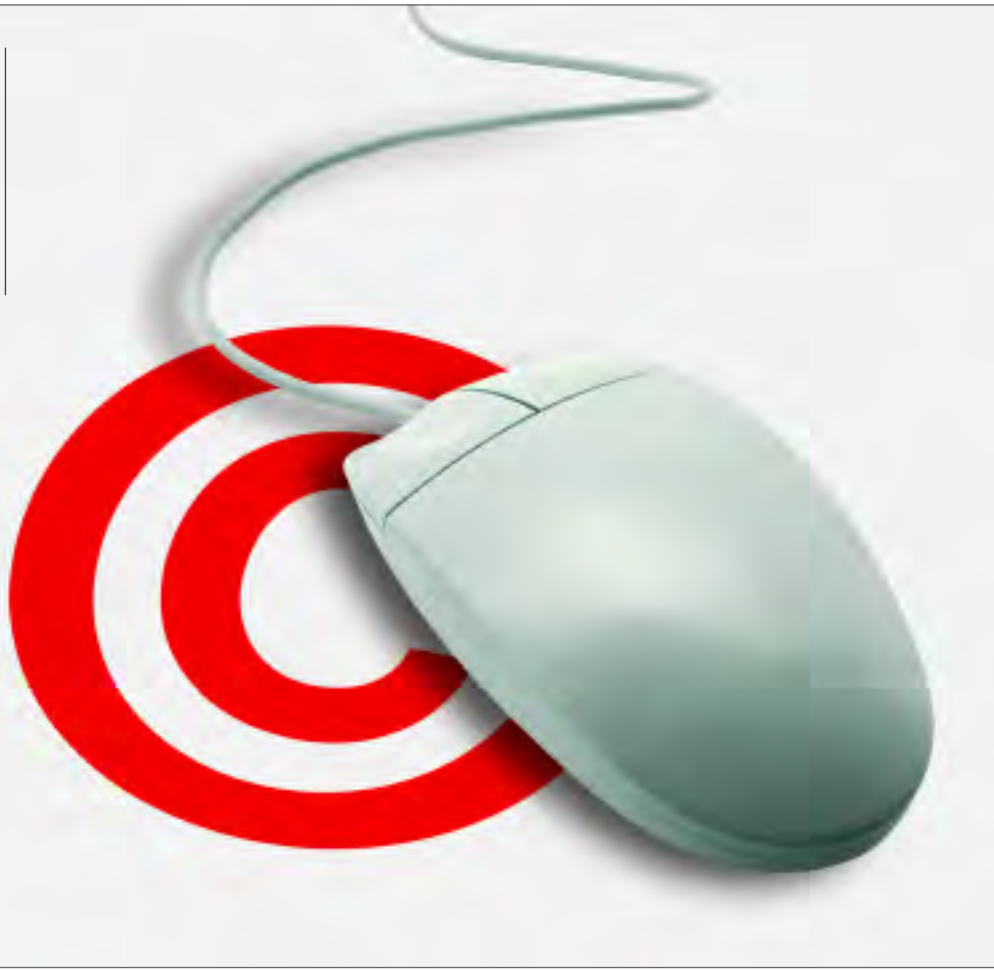
MIPI
MUSIC INDUSTRY PIRACY INVESTIGATIONS

ARIA
AUSTRALIAN RECORDING INDUSTRY ASSOCIATION

You are at risk if commercial music, movies or other copyrighted material is on your organisation's computer systems without payment to, or permission from, the rights owners.

This guide explains what you can do to protect your organisation against the legal and security risks of copyright theft.

CONTENTS©



WHAT ARE THE RISKS?©

Copyrighted music, films and other material should not be copied on your computer systems, or made available on the internet, without permission from the copyright owner.

Copyright protects creative people against this sort of unauthorised copying or distribution of their material, which amounts to theft of their livelihood.

Without adequate precautions, the computer systems of an organisation like yours can become an illegal distribution hub for copyrighted material. This raises a number of legal and security risks for your organisation and employees.

CIVIL OR CRIMINAL LAWSUITS

The laws of virtually every country make it unlawful to copy, distribute or put someone else's material on the internet without their permission. Copyright owners have particular concerns about copyright theft over the networks of public and corporate organisations, given the scale of damage that can result.

That is why copyright and other rights owners regularly take legal action against organisations and individuals that violate copyright on 'file-sharing' and other networks. In June 2005, for example, the music industry found and brought legal proceedings against a medical practice in Germany whose networked computers stored and offered a large number of commercial music files on internet 'file-sharing' services.

The risk of legal action is real: research firm Jupiter found in an April 2004 study that 37% of music 'file-sharers' in the UK have cut down on this activity because of the fear of legal action.

SECURITY BREACHES

If there is unauthorised copyrighted material on your organisation's systems, you may also be running serious risks to your company data, confidentiality and IT security. Illegal websites and unlicensed 'file-sharing' services – the source of much illegal music, film, software and other copyrighted material – are notorious sources of:

Viruses. These destructive elements can crash individual machines and spread through your network. A 2004 study by security firm TruSecure found that 45% of software files downloaded from the most popular unauthorised 'file-sharing' service contained a computer virus, 'worm' or other malicious code.

Spyware. 'File-sharing' software often includes undocumented 'spyware' that reports on computer usage, delivers advertising and other unsolicited files, and can't be removed without substantial time and sometimes computer damage. An NPD Group survey in June 2005 found that 40% of peer-to-peer (P2P) users reported having problems with the amount of spyware, adware and viruses that can be found on these services.[1]

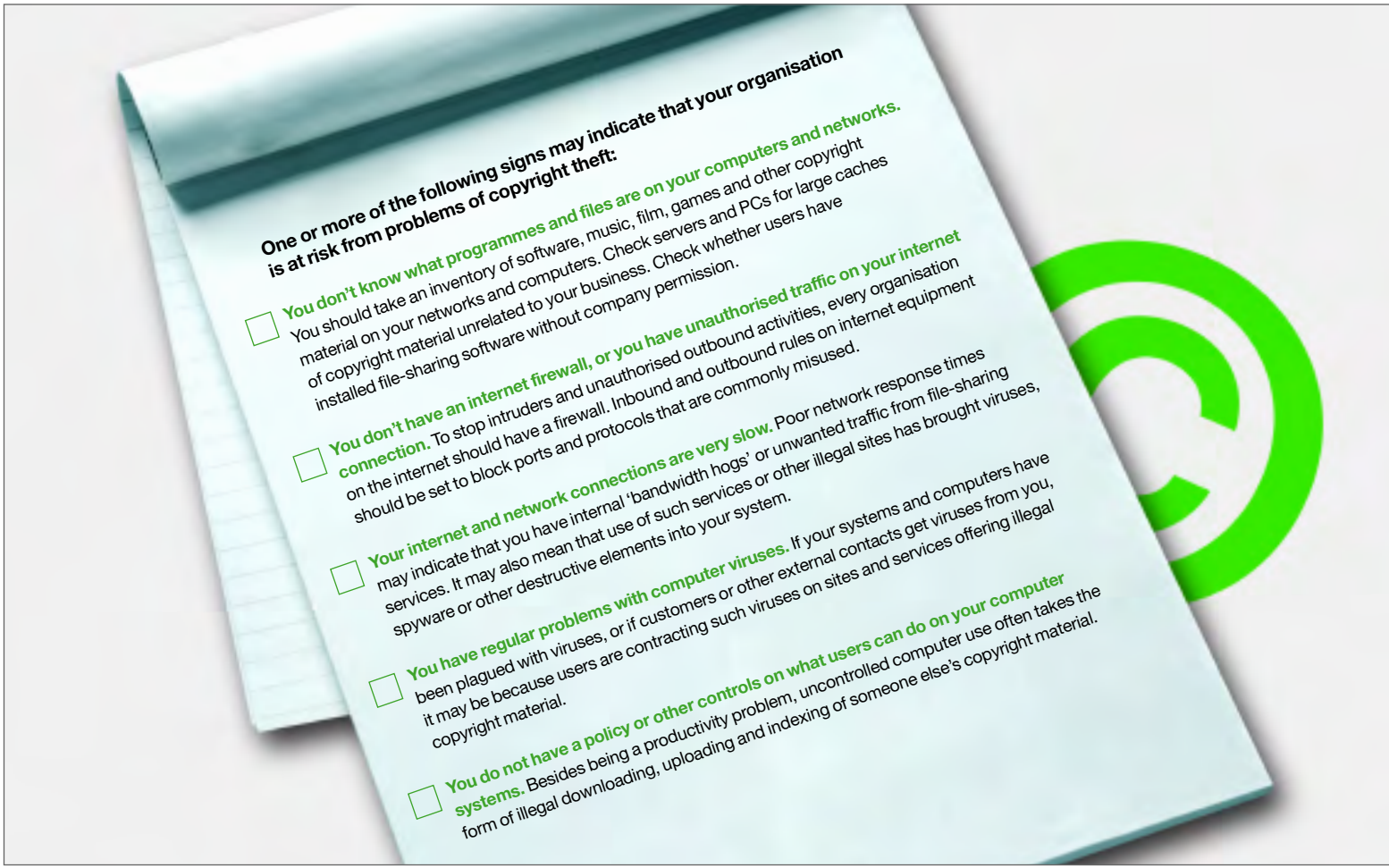
Firewall compromise. 'file-sharing' software typically demands an open port between the user's computer and the internet. This is effectively a gaping hole in the firewall that you are using for network security, and opens your systems to millions of anonymous users.

Resource drains. Unauthorised music and other copyrighted files can use up gigabytes of your server and PC hard discs. 'file-sharing' also lets users both inside and outside your organisation use your system's resources for downloading, uploading and indexing illegal files – which can drain large quantities of your network and internet bandwidth.

[1] Source: NPD MusicWatch Digital, USA, June 2005

One or more of the following signs may indicate that your organisation is at risk from problems of copyright theft:

DO YOU HAVE A PROBLEM?©



There are several practical steps that you can take to avoid copyright theft on your organisation's computers and systems, and prevent the legal and security problems that can result.

WHAT CAN BE DONE?©

SET A COMPANY POLICY

Users, managers and IT personnel need to understand that unauthorised copying and transmission of someone else's music or other works is copyright theft, which the organisation does not condone. This is best implemented in your organisation's policy manual and terms and conditions of employment. A sample memo and policy statement are included in this guide (see pages 6–7 or download a copy from www.ifpi.org or www.mpaa.org).

TAKE COPYRIGHT INVENTORIES

Many organisations already audit their systems for certain types of copyright material, particularly software. Inventories should also include music and other major types of copyright material. Music files are typically 3–5 megabytes in size, stored in .mp3, .wma or .wav format, and often found in \my music or \shared directories. Movie files are typically 500 to 700 megabytes in size, stored in .avi, .mpg or .mov format. These files can sometimes be included in compressed files like .zip or .rar files.

DELETE UNAUTHORISED MATERIAL

Commercial recordings of music and movie DVDs are virtually never licensed for corporate or other multiple copying, or licensed for internet distribution, except through recognised, legitimate services. You should ask for and keep evidence to show that any copies of copyright material are legal.

CONTROL FILE-SHARING

Many organisations ban unauthorised software installations and 'file-sharing' activity on their corporate machines as an easy way of reducing copyright and security problems. Software programmes like freeware Digital File Check can scan for, block or remove file sharing software from personal computers (www.ifpi.org or www.mpaa.org).

SET FIREWALL RULES

Your internet firewall can be configured to screen out infringing files and illicit services in a number of ways. Particular internet addresses, ports or protocols on which 'file-sharing' typically occurs can be blocked. Commercial vendors also offer sophisticated software that can selectively filter copyrighted material.

CONTROL WIRELESS ACCESS

You should be sure that wireless connections to your network and the internet are encrypted and secure, so that these connections are not hijacked for illegal purposes. Wireless hub software lets you set access codes and the desired level of encryption.

WATCH TRAFFIC LEVELS

Network monitoring software, which may have been supplied with your network equipment, allows you to check whether users or devices are hogging bandwidth. Check traffic 'hot spots' to see if there is a system problem or illegal activity taking place.

MAINTAIN VIRUS PROTECTION

Anti-virus software can screen out rogue files containing viruses, spyware or other damaging material, and should be installed on every computer. Vendors update this software regularly to take account of new viruses. You should be sure that all copies of anti-virus programmes are run regularly and kept up to date.

MAINTAIN SPYWARE PROTECTION

Similarly, a range of commercial software programmes can find and remove spyware, adware and similar programmes from your organisation's machines. Anti-spyware programmes should be run and updated regularly.

DESIGNATE A COMPLIANCE OFFICER

Someone in your organisation should be responsible for protecting against copyright theft on your systems. The person needs to be sufficiently senior (such as the IT or finance director) to insist on ongoing compliance with your organisation's policy, to remove illicit material promptly, and to deal with notices and disciplinary actions should they arise.

SAMPLE MEMO©

You can download a copy of this Memo from www.ifpi.org or www.mipi.com.au

MEMO

TO:	DISTRIBUTION LIST)
FROM:	(SENIOR MANAGEMENT OFFICIAL)
SUBJECT:	POLICY ON THE USE OF COPYRIGHT MATERIAL
DATE:	(INSERT)

The purpose of this memorandum is to remind you of (Organisation's) policy on the use of copyright material on (Organisation's) computers, networks and media.

Unauthorised copying and use of copyrighted material is illegal and can expose you and (Organisation) to civil or criminal liability under the copyright law. This applies to all types of copyrighted material, including music, films, games, software and other works.

Employees must not put unauthorised copies of copyrighted material on computers, networks or media owned by (Organisation). Nor should employees put unauthorised copyrighted material on the internet, or engage in activities such as peer-to-peer 'file-sharing' that are likely to promote or lead to copyright infringements.

(Organisation's) detailed policy on the use of copyright material, which includes possible disciplinary actions for failure to abide by this policy, is attached. (Compliance Officer) will be organising regular audits of all (Organisation) computers and networks to ensure compliance and, if necessary, to remove unauthorised items if you have not done so.

Please do not hesitate to contact (Compliance Officer) if you have any questions.

SAMPLE POLICY©

You can download a copy of this Sample Policy from www.ifpi.org or www.mipi.com.au

POLICY ON THE USE OF COPYRIGHT MATERIAL

(Organisation) respects the copyright of those involved in creating and disseminating copyright material, such as music, films, software, and other literary, artistic and scientific works.

(Organisation) employees shall not make, store, transmit or make available unauthorised copies of copyrighted material on (Organisation) systems, equipment or storage media.

(Organisation) employees shall not download, upload, store or make available unauthorised copies of copyrighted material via the internet using (Organisation) systems, equipment or storage media.

(Organisation) employees shall not install or run peer-to-peer 'file-sharing' software or operate a peer-to-peer index or server on (Organisation) systems or equipment, without (Compliance Officer's) consent.

(Compliance Officer) is responsible for carrying out this policy. Any questions as to whether an employee may copy or use copyrighted material in ways covered by this policy should be raised with (Compliance Officer) before proceeding.

Any activities or materials that violate this policy are subject to immediate removal, termination and/or forfeiture of the material.

(Organisation) employees that violate this policy are subject to discipline as appropriate under the circumstances. Such discipline may include termination.

_____

Employee signature and date

ARIA
AUSTRALIAN RECORDING INDUSTRY ASSOCIATION

MIPI
MUSIC INDUSTRY PIRACY INVESTIGATIONS

Australian Recording Industry Association

Level 4, 19 Harris Street,
Pyrmont NSW 2009

Tel: (02) 8569 1144
Fax: (02) 8569 1181
www.aria.com.au

Music Industry Piracy Investigations

PO Box Q20
Queen Victoria Building
NSW 1230

Tel: (02) 8569 1177
Fax: (02) 8569 1181
www.mipi.com.au

Published by IFPI, September 2006

Designed by elliottyoung +44 (0)845 054 0070