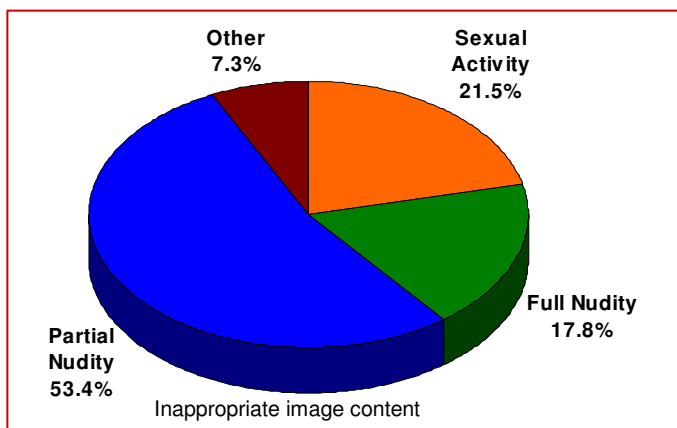


No Nudes is Good News

Andy Churley, director at PixAlert looks at the problem of preventing inappropriate & illegal images in corporations

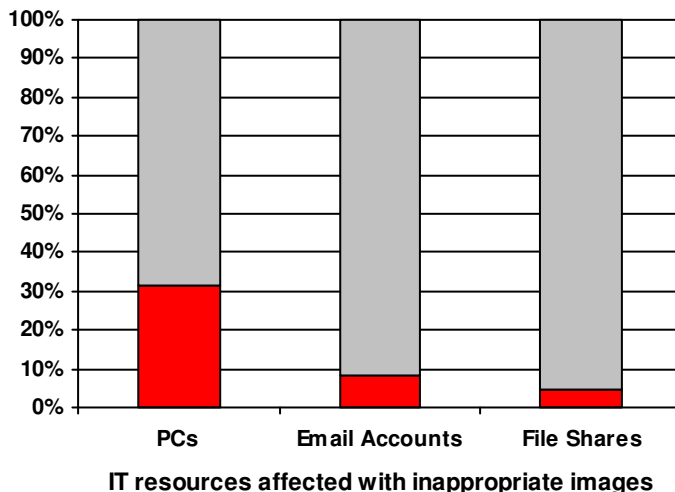
Recent statistics collated during 60 corporate audits undertaken by PixAlert between June and September 2006, found that 31.2% of the 5,000 PCs scanned contained digital pornography or other inappropriate images, 8% of the 5,000 email server accounts and 4.5% of 10,000 file server shares scanned were similarly affected. These figures support the recent Audit Commission's findings that 47% of reported IT incidents is for accessing inappropriate material.

This may be no surprise to the seasoned IT security professional; who understands the most difficult IT security threat to prevent is that of an 'insider attack'. Those downloading and distributing inappropriate content will happily ignore corporate policies and will go to extraordinary lengths to bypass corporate protection systems in order to obtain material which, while maybe titillating or amusing for some, more often than not causes offence and distress to those who receive it inadvertently and leaves a latent threat to the corporation inside their defences..



Corporate officers, who have a clear understanding of reputational risk but little experience of IT security, wrongly assume that boundary protection systems will prevent any digital pornography from entering the network.

Unfortunately, there are a myriad of ways that illegal or inappropriate images can get on to the desktop and corporate network other than via the Internet. Typically, a computer will have conventional points of entry such as CD/DVD, Ethernet card, serial and parallel ports; modern connectivity protocols such as USB have opened computers up to multiple new hardware devices with very high data transfer rates. The ability to plug and play using USB has meant an extremely rapid introduction of storage devices such as portable hard drives, PDAs, USB Keys, mobile



phones and media players that are very hard for corporations to control.

Unmonitored web activity on computers and PDAs at home is now widespread. This is a situation that will only get worse with the rise in easy instant connectivity to WiFi hotspots and broadband at home. In addition, peer to peer communications, encryption of transmitted data and secure internet connections will all bypass or compromise any corporation's gateway filtering solutions. The majority of corporations currently rely solely on image protection at the internet gateway that works by blocking traffic from a banned list of sites or filters out spam emails. But the mere fact that 20,000 new pornographic web pages are launched per day means that it is impossible to keep an up to date list of harmful sites. Such systems, while an essential part of any IT defence solution, can do nothing to counteract increased threats from new technologies such as PDAs, memory sticks, DVDs CDs, digital cameras and camera phones.

Legislation

Worryingly, in many jurisdictions, corporate officers are largely unaware that they and their companies could be held criminally and civilly liable if illegal images are found on corporate computers. Put simply, there can be huge legal, financial and reputational implications for the corporation and its officers if they do not take appropriate measures to ensure illegal and inappropriate images are not stored on corporate computer systems. Irrespective of any legal penalties, adverse publicity can have a detrimental effect on a corporation's reputation which can affect trading performance.

How to 'cover-up' without a 'cover-up'

The sheer quantity of images found during audits emphasises the fact that policies and gateway security technologies alone are not sufficient to prevent inappropriate and illegal images in the workplace.

Corporations are turning to Auditing and Monitoring corporate IT assets in order to help manage this growing issue.

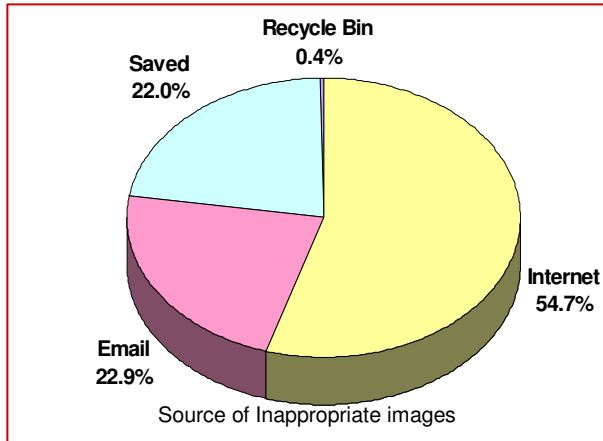


Image auditing is the preferred route of many corporations and software solutions exist which will scan IT systems for illicit image content held in static files on corporate IT resources. One advantage of image auditing is that no software needs to be deployed on target machines; one disadvantage is that encrypted or password protected files cannot be analysed.

Screen monitoring is often restricted to 'high risk' IT assets such as laptops which are rarely connected to the corporate network. Screen monitoring detects illicit images while they are being viewed on the computer screen. One advantage of screen monitoring is that it is 'always on' monitoring 24 x 7; one disadvantage is that a company must manage a software deployment to all target PCs.

Whichever method is used, three phases are usually employed:

- Discovery;
- Categorisation;
- Reporting.

Discovery: Software solutions use advanced algorithms to provide a statistical likelihood that an image contains illicit material. If an image transgresses a threshold level then it is returned to the auditing or monitoring application for review.

Categorisation: automatic classification of known illicit images, an auditor will review the remaining suspect images for illicit content.

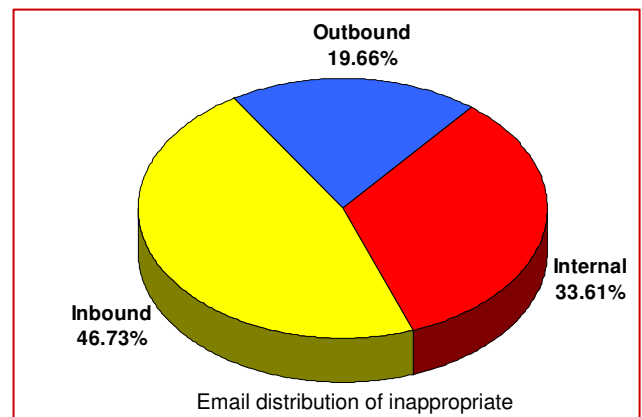
Reporting: automatically generated reports which provide sufficient information for a disciplinary decision to be taken without displaying the image (to prevent potential distress to those viewing the image)

or identifying the target (to prevent any prejudice during or after the disciplinary process).

A change in culture is needed

Almost all corporates will say they actively discourage access to inappropriate images. They back this up by pointing to the corporate acceptable usage policy and the implementation of boundary protection systems. However, the reality is that almost all establishments, whether they are public limited companies, privately owned companies, central government departments or local government authorities, educational establishments, hospitals, not for profit organisations or religious groups, will have digital pornography residing on their corporate IT assets.

Many companies act by sending out warnings that this sort of behaviour will not be tolerated. PixAlert's experience is that this achieves little or nothing.



The only way to eradicate illicit image abuse in the workplace is to change the corporate culture; no amount of corporate policies and vocalisation will change it without strong policy enforcement. Nowadays, companies cannot afford to just 'talk-the-talk' they must 'walk-the-walk'. Acceptable levels of behaviour should be clearly defined; penalties for breach of corporate policy should be well understood and staff should know that the organisation is actively auditing or monitoring corporate IT assets and such penalties will be brought to bear on anyone caught breaching policy.

At the same time staff should be fully aware of what actions to take if they accidentally receive, view or uncover inappropriate image material.

About the Author

Andy Churley (BEng, CEng, MBA, MBCS, CITP), is a director at PixAlert and has over 17 years experience in the fields of IT security, knowledge management and organizational structure and culture.

PixAlert International
Digital Hub
10-13 Thomas Street
Dublin 8, Ireland

Tel: +353 1 707 8860
Fax: +353 1 707 8861
Email: info@pixalert.com