

# Image Analyzer

## Email Health Check

Most companies now recognise email content filtering to be an essential element of perimeter security. It allows corporations to enforce their email acceptable use policy at the gateway; providing protection against viruses, spam, phishing, dangerous file types, inappropriate language while educating users on appropriate email usage.

However, nearly every email policy contains a clause that few email content filtering applications are setup to enforce. This clause expressly states that the email system is not to be used for the distribution of pornographic content - yet pornography continues to travel in and out of corporate email systems hidden within the mass of legitimate business images.

These pornographic images constitute a real threat to the business with the risk of legal liability, sexual harassment lawsuits and damaged company reputation.

### The Issue

The issue is not unsolicited pornographic spam but social communication between friends and colleagues who do not understand the possible repercussions, or do not care.

Employees may think that their work email is a private form of communication but this is not the case. A single email can rapidly spread beyond its intended destination both internally and externally. If that email contains sexually explicit content there is a high probability that at least one of the recipients will find it offensive. Unchecked email can damage the company culture and contribute to the creation of a hostile working environment.

### What is sexual harassment?

*"Sexual harassment is unwelcome behavior of a sexual nature."  
UK Equality and Human Right Commission*

Sexual harassment can take various forms which include sexually explicit emails, sexually explicit pictures and accessing sexually explicit internet sites.

Any of the following may count as sexual harassment:

- The display of pornography
- The circulation of obscene material (by email, for example)
- Any unwelcome behavior of a sexual nature that creates an intimidating, hostile or humiliating working environment.

### In the Press

2.5 billion (8% of total emails) are pornographic

70% of employees admit to viewing or sending adult-oriented personal e-mail at work.

(NFO Worldwide)

27% of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems.

(American Management Assoc.)

DVLA (Drive & Vehicle Licensing Agency) dismissed 14 staff following email pornography

(BBC News)

Merrill Lynch sack 13 staff due to inquiry into sending pornographic emails

(ZDNet)

Audits on over 125 corporate and public sector networks over the last nine months found that 25.8% of the 10,000 PCs scanned contained digital pornography or other inappropriate images.

### *What are the legal obligations of an employer?*

"All employers have a duty to protect their employees from sexual harassment, and they can be held liable for the unlawful action of those who work in their organisation." *UK Equality and Human Right Commission*

Employers are "vicariously liable" for acts of sexual harassment committed by their employees under the Protection from Harassment Act 1997 unless they have taken all reasonable steps to prevent it from taking place.

To take all reasonable steps, at a minimum an employer would be expected to have an appropriate email acceptable use policy which is effectively **enforced, monitored** and **communicated** on an ongoing basis.

A written policy on its own is insufficient. A policy that is not implemented through communication, education and enforcement will be of little or no use in discharging liability.

### *What are the risks of ignoring the threat?*

Saying "I'd rather not know" and ignoring the threat can have repercussions which could even extend to criminal charges against the employer if illegal imagery is involved. By taking proactive measures to monitor, educate and enforce policy the employer can significantly mitigate the risks of:

- |   |  |  |
|---|--|--|
| <ul style="list-style-type: none"><li>• Damaging company reputation and brand</li><li>• Fostering a hostile working environment</li></ul> |  | <ul style="list-style-type: none"><li>• Sexual harassment lawsuits</li><li>• Criminal lawsuits</li></ul> |
|---|--|--|

## **The Solution**

The Image Analyzer anti pornographic image scanner allows organisations to protect themselves from this threat. It allows organisations to enforce, monitor and communicate their email policy in relation to the distribution and exchange of sexually explicit email attachments.

### *Technology*

Image Analyzer provides the technology to differentiate pornographic images from the mass of legitimate business images traveling through the email gateway on a daily basis. It uses sophisticated real time composition analysis to reliably distinguish between pornographic and non pornographic images. Once the image has been identified as suspect it records details such as the sender, recipient, date and time.

### *Education*

Once the sender has been identified, an optional automatic email notification can be sent stating that the email has breached the email acceptable use policy. This process educates the parties involved that this type of communication is unacceptable and that the business has a means to identify it.

### *Monitoring*

The email details can be logged to a reports database for review by HR on a regular basis. These reports give the organisation clear visibility of the level of misuse and the parties involved.

## **Email Health Check**

The first step to protecting an organisation is to determine the current health of the email communications. Image Analyzer offers a free 30 day email health check to provide business intelligence which details the quantity of high risk images being distributed through the email gateway. It gives management complete visibility of the level of misuse within their organisation and allows them to decide the best course of action to resolve any resultant issues.

The email health check is a non-intrusive audit of the images being distributed via the corporate email system. During the audit no emails will be blocked and no notification will be sent, the technology will only log information for reporting purposes.

At the end of the audit a detailed report will be supplied and access provided to copies of any high risk communications for further assessment.