e-mail and web usage

Dependence brings better governance

In the 2004 survey, Internet usage had climbed to 93% of UK companies. The late adopters tended to be less controls-conscious. As a result, incidents of staff misuse rose rapidly.

This survey shows even higher levels of adoption; 97% now have an Internet connection and 88% of these are broadband. With broadband, the Internet is only a click away.

Increasingly, UK businesses recognise the temptation this poses to their staff. More companies have an acceptable usage policy for the Internet than have an overall information security policy. The dip in controls seen two years ago has reversed.

Telecommunications and technology companies are most likely to have an acceptable usage policy. Leisure, retail and property companies are least likely.

Companies with a policy are nearly three times as likely to have reported staff misuse as those without. Those without tend not to have a clear corporate view on what constitutes misuse, so do not pick up all incidents.

Three quarters of companies with an acceptable usage policy require staff to acknowledge that they have read it before they can access the Internet. This proportion has grown over the last four years, particularly in small companies.

Companies that have experienced staff misuse in the past are most likely to restrict Internet access.

Misuse levels stabilise

After the sharp rise two years ago, staff misuse of the Internet has levelled off.

In how many UK businesses did staff misuse e-mail or web access?

Larger companies are more likely to have incidents involving staff misuse. Every very large respondent had at least one incident of this type in the last year.

Web misuse dominated the worst incidents involving staff. 41% involved staff accessing inappropriate web-sites; a further 36% related to excessive web-surfing. The most serious of these involved access to illegal material; several companies reported incidents of staff accessing child pornography.

One of the staff at a small services company accessed adult web-sites at work. He used someone else’s computer to conceal his activity.

The average cost of individual staff misuse incidents was relatively low compared with other types of security incident. Less than 10% of staff misuse incidents caused business disruption or direct cash costs. Many simply wasted time.

A lovesick employee at a medium-sized manufacturer spent up to six hours a day on a dating agency web-site.

What hurts companies is the number of these incidents they suffer, more than one a day on average. While the median was only a few incidents a year, some small companies reported hundreds of e-mail abuses every day.

Technology, telecommunications and utility companies were most likely to report incidents; retail and travel were least likely.
The information security breaches survey has over the last decade formed an integral part of the DTI’s programme to help UK businesses address the issue of information security.

The survey takes place every two years and involves telephone interviews with 1,000 businesses of all sizes across all areas of the UK, plus a series of face to face interviews and interactive surveys.

Based on the total sample of UK businesses in this survey, we are 95% confident that the margin of error for our sampling procedure and its results is no more than +/- 3%.

The 2006 survey was managed by PricewaterhouseCoopers for the DTI and was sponsored by Microsoft, Clearswift, Entrust and Symantec.

For more information, please refer to the Information Security Breaches Survey Technical Report (URN 06/803). This is available from 25 April 2006 and can be downloaded from www.security-survey.gov.uk

### Improved technical controls

Scanning incoming e-mail and web downloads has become common, especially in large companies.

### What technical controls do UK businesses have over their staff’s Internet access?

<table>
<thead>
<tr>
<th>Control</th>
<th>ISBS 2006 - large businesses</th>
<th>ISBS 2006 - overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block access to inappropriate web-sites</td>
<td>74%</td>
<td>74%</td>
</tr>
<tr>
<td>Log and monitor web access</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>Scan incoming e-mail and web downloads for viruses</td>
<td>94%</td>
<td>94%</td>
</tr>
<tr>
<td>Scan web downloads for spying</td>
<td>78%</td>
<td>78%</td>
</tr>
<tr>
<td>Filter incoming e-mail for spam</td>
<td>80%</td>
<td>80%</td>
</tr>
<tr>
<td>Block or quarantine e-mail attachments</td>
<td>30%</td>
<td>30%</td>
</tr>
</tbody>
</table>

Companies that log and monitor web access reported more incidents than those that do not; content security tools play a key role in detecting abuse.

There has been a big increase in the proportion of UK businesses that filter incoming e-mail for unsolicited messages (“spam”). Two-thirds of the businesses that do not scan incoming e-mail for viruses do filter for spam and block suspicious attachments.

### Reputation is critical

Protecting the organisation’s reputation is one of the most important drivers for information security. 90% of all companies say this is important. It is an even bigger priority for large businesses; 72% say it is very important.

Mass-messaging viruses have made UK companies recognise the danger of e-mailing a virus to their customers. As well as their reputation suffering, litigation could follow. Two-thirds, therefore, scan outgoing e-mail for viruses. Generally, the companies scanning outgoing messages are a subset of those that scan incoming ones.

A company’s reputation can also suffer if its staff (either deliberately or by mistake) send offensive correspondence to customers. This is especially true if the media report the story, as has happened in several recent cases.

### Accidental misuse can be as damaging as deliberate.

Staff at a medium-sized manufacturer e-mailed confidential information to the wrong company by mistake.

Protecting confidential information sent by e-mail as it passes across the Internet is still rare. In only a quarter of UK businesses can staff send encrypted e-mail to the company’s main business partners.

Roughly one in five UK companies allows staff to download free auto-address software onto their PCs. Such software often stores confidential information (such as e-mail addresses) on a third party’s servers. Most users are not considering the security risks this poses.

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2006. URN 06/806.

Clearswift simplifies content security. Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic. Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service. Twenty years of experience across 15,000 organizations has helped us raise security standards while simplifying security management.

For more information, see www.clearswift.co.uk.