Almost every business now uses the Internet

The trend towards Internet usage that we saw two years ago has continued. The vast majority of UK businesses with a computer now use the Internet. E-mail remains more common than web browsing, but the gap is closing.

Indeed, for many organisations, it is hard to envisage doing business without e-mail and the web. E-mail tends to be cheaper and faster than sending a letter. It also is sometimes more convenient than playing telephone tag. The web provides access to almost limitless information.

One medium-sized company commented that e-mail used to be internally focused and non-essential. It has now become a critical element in communicating with customers, and now figures highly in its business continuity plans.

Unfortunately, as with any new technology, there is a downside. Many web-sites provide content that is inappropriate to most businesses. From offensive jokes to cyber-terrorism, you can find it all on the Internet. Some is merely discriminatory. Other content, such as child pornography, can result in criminal proceedings.

Staff members who download inappropriate material tend to share it by e-mail. Before you know it, your business is sending illicit material to other organisations. The risk of a damaged reputation is significant.

Finally, even “harmless” web browsing can consume a disproportionate amount of staff time.

Internet abuse is on the rise

Roughly one in five UK companies suffered from staff abuse of the Internet in the last year. Over half of all large companies were affected. These numbers were significantly greater than staff misuse of other systems.

Companies that experienced Internet abuse tended to have many such incidents during the year, on average one a week. Interestingly, those small companies affected had roughly as many breaches as large ones, despite having fewer employees.

8% of companies said their worst security incident of the year involved staff misuse of the Internet. Roughly one in five had a very serious impact. Excessive personal e-mail and access to inappropriate web-sites were the two biggest causes.

A few incidents caused customer complaints. For the rest, the main impact came from disruption to the business during the investigation. Over half involved major disruption. The typical investigation lasted up to a week and involved on average 1-3 man-days.

While most of the effort was internal, some companies spent a few thousand pounds on specialist advice. Direct financial loss (e.g. compensation payments) as a result of Internet abuse was rare.

DTI recommends

- Have a clear policy on what your business considers to be acceptable usage of the Internet.
- Communicate this policy to your staff.
- Implement software to monitor Internet usage and block inappropriate web-sites.
- Have a clear contingency plan for what to do if an incident arises in your business.

For more information, please see www.dti.gov.uk/industries/information_security

Information security breaches survey 2004

Staff misuse of the internet
Websense, Inc. (NASDAQ: WBSN), the world’s leading provider of employee Internet management solutions, enables organizations to optimize employee use of computing resources with Web filtering in addition to mitigating threats related to Internet use including instant messaging, peer-to-peer, and spyware. By providing usage policy enforcement at the Internet gateway, on the network and at the desktop, Websense Enterprise enhances productivity and security, optimizes the use of IT resources and mitigates legal liability for our customers. Websense, awarded Forbes Magazine’s 2004 “Top 25 Technology Companies,” serves more than 20,000 customers worldwide, representing 16.4 million seats. For more information, visit www.websense.com.

Controls over Internet abuse have relaxed

Part of the reason for the increase in number of companies reporting Internet abuse incidents is that more businesses provide their staff with access than two years ago. However, this is only part of the answer. Worryingly, it appears that fewer businesses on average have controls over their staff’s Internet access than in 2002.

Learning from incidents

Only one in three companies suffering an incident involving Internet abuse had a contingency plan in place to deal with such incidents. However, where plans were in place, most proved to be very effective at handling the incident.

For e-mail, quarantining attachments seems to reduce the likelihood of having any incidents. However, it also increases the number of incidents significantly, with businesses often handling hundreds of false positives. Some businesses have found this very time-consuming. This may explain why far fewer quarantine now than two years ago.

Companies that have restricted staff access and put policies in place tend to have significantly fewer e-mail abuse incidents. With web abuse, the pattern was less clear, but there does seem to be a slight reduction.

Companies logging and monitoring web access reported a higher incidence of Internet abuse. This implies that among those organisations without this control, similar incidents are going undetected.

For more information, please refer to the Information Security Breaches Survey Technical Report (URN 04/617). This is available from 27 April 2004 and can be downloaded from www.security-survey.gov.uk.