The dark side of the web

End-users who are either ignorant or curious about IT are at least as big a risk to companies as criminals – which means IT professionals must be constantly alert to both obvious and unlikely threats: that was the message from a recent BCS annual lecture

BECOMING A computer criminal or exposing an organisation to risk – maliciously or inadvertently – is as easy as making a few mouse clicks; this was demonstrated live at the annual lecture organised by the BCS and the Royal Signals Institution. The trouble is that this means company systems are potentially under threat from anyone with a PC, either inside or outside the organisation.

'Systems would run perfectly if only we didn't have users,' said Colin Rose, a security, legal and business management expert who is now consulted by government agencies and companies worldwide after researching IT security issues for several years.

'We show users how to do things but they do it their way. They change things. They install their own programs and games. You can't configure a user like you can a PC: they just do what they want.

'But users are the reason we have IT. IT is a chunk of tin: servers, routers, hubs; the reason it's there is information systems. Information systems are about people putting information in, having it stored and processed and taken out. We have to make sure users understand the value of what they have in their information systems and the consequences of what they do. In addition, users can be your best ally: they spot problems.'

He pointed to surveys showing that 60% of IT security breaches come from inside organisations – and these breaches are not necessarily malicious, but their impact can be far reaching.

'If someone's accessing lewd images there's a productivity issue: that person is not doing their job,' he said. 'If it's child pornography it's a criminal issue: the police could knock on the organisation's door because of one individual, bringing bad publicity and lost reputation. Another user could see the images and feel harassed; they might leave and claim compensation, costing the organisation money and, again, reputation – and the organisation loses the wrong person, the person who is actually doing their job properly. All this is activity by people inside the organisation.'

Information can be disclosed inadvertently, Colin Rose said. He highlighted a feature in Microsoft Word which can save apparently deleted text and document owner information in the final version of a file.

The information is hidden but can be viewed with a simple software utility, potentially causing embarrassment or worse if the file is sent to a customer or supplier. For example a document file might include copyright information from another organisation, such as contract terms – and could show the details of the originator. Or there might be insults against the recipient, or notes about negotiating techniques to be used with this customer, included in earlier circulated copies but apparently deleted from the final document (see separate panel).

Public PCs, for example in hotel rooms, can reveal information about their previous users. Colin Rose mentioned real cases of such PCs revealing details of online chat between married lovers, and access to pornography websites, leaving the users open to blackmail. Exploring the cache on a PC in a hotel room could also throw up emails with details of business deals. The new user could call the company and appear genuine, using the confidential information in the email, and change the deal.

Information on everything from making bombs to robbing bank cash machines and killing people is readily available online, Colin Rose showed. The guide to killing people has been used in real murders, he said.

He called up an online guide on how to pick locks – put on the web by none other than the Massachusetts Institute of Technology.

Even if information published on the web maliciously or by mistake is taken down, it is potentially there for access forever, Colin Rose said: there are sites which keep copies of all websites, so users can find previous versions or sites that have been removed.

'Once you publish on the web, it's out there,' he said. 'You can't unpublish on the web.'

He accessed and demonstrated online utilities

'We show users how to do things but they do it their way. They change things. They install their own programs and games. You can't configure a user like you can a PC: they just do what they want.'