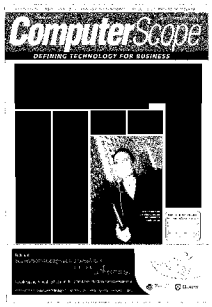
Publication: Computerscope
Date: Wednesday, November 22, 2006
Page: 1
Extract: 1 of 2
Circulation: 9.681
Author:
Headline: Irish organisations failing on device control



Irish organisations failing on device control

Digital devices running rampant in corporate networks, says survey

A POLL OF *ComputerScope's* readership has shown that Irish organisations are struggling to control digital devices among staff. A question in the poll asked if staff in organisations used personal digital devices that they had acquired themselves to connect to computers or the network. While the majority at 58% said no, a worrying 36% said that such devices were in use.

Conor Flynn, technical director, Rits, said that there are many problems around technology self-enablers that can expose organisations to legal action.

"Through the media, organisations are becoming aware of the problems with these devices around Digital Rights Management (DRM), though they are still slow to put products in place to control them." Flynn gives the example of a mobile phone that has music stored on it. Whereas the user may have acquired that music legally on the device, if it is backed up to a corporate PC, then it is now on a machine for which it is not licensed. "The big thing is that the corporation is open to being sued under the copyright act for digital rights abuse, even if it is an employee that is doing it," said Flynn.

Flynn went on to say that there are other examples of legal liability with such devices. He highlighted the example of where an employee may have social photographs taken during a night out, or perhaps even in a more intimate setting. Were such photographs to be then synchronised to a corporate machine, there may be the threat of not only inappropriate but also of illegal material.

Flynn went on to say that the failure to recognise the capabilities of such devices can also be a problem. "A lot of people are becoming more aware of the issues around portable media, but there are still problems in recognising them. For example phones today have cameras in them, but some have memory cards in them and appear as a drive letter when you connect them to a PC," explained Flynn. "We are seeing companies saying you can't use an Ipod, or a flash disk, but often there is nothing around mobile phones."

Paul Moylett, operations director with Topsec Technologies, said that the types of devices that many organisations provide to staff could be contributing to the problem. "Companies will buy mobile phones at a basic level – it's a phone, it works and it makes and receives calls – but most people, on their private phones or PDAs, may have way more advanced capabilities and they will want to synchronise them with their appointments and contacts."

A further question in the survey asked if organisations had a policy around the use of devices such as digital cameras, digital music players and flash memory devices. Here, the majority, 58%, said that no such policy was in place, with a further 4% saying that they did not know if one existed. This would indicate that there is a clear failure among Irish organisations to keep up with developments by ensuring that policies are in place to prevent unwanted data or malicious content entering the network, but also sensitive or confidential information leaving the network. Conall Lavery, managing director, Entropy, agreed that there was a problem but was surprised by the result. "I might have expected a higher 'no' rate on that specific policy. For e-mail policies and internet usage policies, there tends to be a higher rate than for these types of devices. Organisations, in our experience, are really beginning to realise the threat."

The full report on the survey can be seen on page 39 of this issue.

Publication: Computerscope
Date: Wednesday, November 22, 2006
Page: 1
Extract: 2 of 2
Circulation: 9.681
Author:
Headline: Irish organisations failing on device control