

A yellow banner for Workhound. On the left, a woman in a white shirt and black vest is looking at a laptop. In the center, a white speech bubble contains the text "An Extra £15k?". To the right, the "workhound" logo is displayed in blue and white, with a small dog icon. Below the logo, the text "If your dream job is out there, we'll find it. WorkHound. THE Job Search Engine." is written. At the bottom right, there is an orange button with the text "click here".

An Extra £15k?

workhound

If your dream job is out there, we'll find it. [WorkHound. THE Job Search Engine.](#) [click here](#)

If this page does not print out automatically, select **Print** from the **File** menu.

Risky behaviour still looms large

Employees ignoring and sidestepping company policies

Shaun Nichols in San Francisco, vnunet.com 22 Oct 2008

Many employees are continuing to behave in a way that puts company data at risk, according to a recent study.

The survey commissioned by Cisco asked a number of employees in the Americas, Europe and Asia about their general computing practices in comparison to their company's IT policies.

The study found that potentially risky behaviour, such as downloading files for personal use or deliberately modifying system security settings, remains prevalent among users.

Around 14 per cent of notebook users deliberately alter the security settings on their company machines. The numbers were highest in China and Brazil, while figures in the UK and US were lower than the average at nine per cent and two per cent respectively.

Gaining web access was the reason most commonly given among those who had altered security settings. Just over half said that they had altered the settings in order to view a web site which was normally prohibited by company policy. Second on the list was privacy concerns, cited by 35 per cent of users.

Around a third of users admitted to allowing a co-worker to use their computer unsupervised, while 13 per cent let a family member access their system.

The survey found that IT administrators are generally aware of the problem, although few are worried about the risk of data loss.

On average, 55 per cent of IT decision makers believed that employees were running unapproved applications on company machines.

However, 24 per cent believe that unapproved programs did not account for any data leaks, while 53 per cent believe that the behaviour accounted for less than a quarter of leaks.

Unauthorised access is not a major concern for administrators either. While 40 per cent of IT decision makers have had to deal with employees gaining unauthorised access to a system, 53 per cent reported having to deal with such situations only a few times a year, and 35 per cent needed to address the issue once a year on average.

Permalink: <http://www.vnunet.com/2228755>

www.vnunet.com/2228755

This article was printed from the vnunet.com web site

© Incisive Media Ltd. 2008

Incisive Media Limited, Haymarket House, 28-29 Haymarket, London SW1Y 4RX, is a company registered in the United Kingdom with company registration number 04038503

[Close](#) this window to return to the website

A yellow banner for Workhound. On the left, a woman in a white shirt and black vest is looking at a laptop. In the center, a white speech bubble contains the text "An Extra £15k?". To the right, the "workhound" logo is displayed in blue and white, with a small dog icon. Below the logo, the text "If your dream job is out there, we'll find it. WorkHound. THE Job Search Engine." is written. At the bottom right, there is an orange button with the text "click here".

An Extra £15k?

workhound

If your dream job is out there, we'll find it. [WorkHound. THE Job Search Engine.](#) [click here](#)