

Virtual assets security in focus

<http://archive.gulfnews.com/articles/08/09/30/10248646.html>

09/30/2008 06:20 PM | By Carole Spiers, Special to Gulf News

Workplace security has shifted its emphasis from physical break-ins and employee theft to the more important, but invisible, threat to sensitive electronic data.

To most employees, the modern science of data-security is something daunting in its scale, complexity and speed of change. They often feel quite confused by it, and conclude that it would take years to learn it all. So they tend not to try. If they haven't been involved in a security breach, they just feel relieved, and trust the data security specialists to handle the situation.

These data security specialists are, of course, a new and important breed of managers, and the recruiting of the best applicants in this category is a major management priority.

But there is clearly a much wider agenda involving the entire workforce - how to encourage all employees to adopt daily work practices that reduce the risk of compromising security, the consequences of which may be disastrous.

A couple of weeks ago, in London, a top company has had a multi-million pound contract cancelled by the government because it was lax in its security and lost a USB drive containing the names and addresses of thousands of government employees.

It is accepted that most of the big security blunders we read about are caused not by hackers but by ordinary staff ignoring security processes, either deliberately or through carelessness. It is terrifying to think what damage can be done by just one person divulging their password over the internet.

All this points to need to basic information security training for staff.

Managers should maintain a strict attitude of security awareness throughout their department. Any employee, who is granted access to sensitive information, should be given formal induction training in information security.

When recruiting new staff, the job-descriptions, background checks and terms of employment should all include a tightly drawn-up confidentiality agreement. The terms of employment should spell out the mandatory regulations in detail.

I worked with a woman in publishing who retired to live in the country. Her employer had forgotten to ask for the return of all the data-assets to which she had previously had access - including the names, addresses and phone-numbers of the top 20,000 earners in the UK.

That material could have been worth a lot of money to the mailing houses and she received an uncomfortable visit from the firm's security chief at her retirement cottage, where she was told that she needed to prove her innocence of data piracy.

When terminating any employment contract, managers should supervise the return of all information assets before departure. This should include a full inventory of the organisation's hardware, software and data media in the outgoing employee's possession, as well as access rights to all information resources and processing

facilities.

- The writer is a BBC broadcaster and motivational speaker, with 20 years' experience as CEO of Carole Spiers Group, an international stress consultancy based in London.