

Pulling the Plug on Data Leaks



In our August Brief Update we looked at the Government's bid to introduce greater penalties for those deliberately misusing personal data. This month we carry on the personal data theme but bring matters nearer to home and consider how you can prevent data leaks from your business or inappropriate use of data by your staff.

From lost lap tops left on the train or plane to carelessly sent emails brimming with sensitive information to circulation of defamatory chain emails - most businesses have experienced a data loss or misuse scare.

Here are some simple steps to stem the flow and plug the gaps:

- **Train your staff** - they are a business' greatest asset but often the most overlooked, to the peril of those in charge. Ensure individuals are screened at the employing stage and ensure employment or consultancy contracts set out clearly what is expected by way of confidentiality obligations. Having put those two building blocks in place, ensure everyone, from the most senior officer to the office junior, receives regular training and reminders about email content, avoiding loose talk and other company procedures designed to prevent mishaps. Reinforce this training with policies and

handbooks which set out clear rules and guidelines designed to be workable in practice - don't simply ban all personal email and internet visits - this is more likely to be honoured in the breach and call the whole policy into question.

- **Secure your equipment** - PCs and laptops can be a major source of loss when firewalls, anti-virus software and anti-spy ware software are not up-to-date. Lap tops are often used to store sensitive information despite prohibitions, so consider encryption, preferably whole drive encryption. At a more basic level ensure filing cabinets are kept locked and confidential papers are not left lying about. Check permissions to ensure access to private documents or email accounts have not inadvertently been allowed.
- **Use available resources** - there is a wealth of products on the market to prevent data loss and information leaks. Consider Content Monitoring and Filtering (CMF) which monitors all the outbound traffic on your network and can alert you to or block certain activities, such as files being emailed to the wrong person. If you have an important database think about Database Activity Monitoring which can observe your database and generate alerts for unusual activity to limit outside attacks and highlight insider misuse.

Lastly, consider the scale of the workplace and personal security risks revealed by the recent report (IT Week 28 November 2006) that over 8,000 laptops/PDAs were left in the back of London's licensed cabs over the past 6 months. With the office party season now in full swing don't be one of these this Christmas!

Season's Greetings from the Intellectual Property & Technology Team and our good wishes for a successful 2007.

For more information on data security issues contact LFCameron@Paull-Williamsons.co.uk