

Infosecurity Europe 2008

Preventing careless data breaches – who's responsible?

*By Nick Hughes
Business Development Manager
3M Optical Systems*

Stories of 'yet another IT security lapse by company X' are hitting the headlines far too often, each time raising the alarm about how little is being done to protect commercially sensitive data on mobile devices and the hidden costs associated with this negligence. Some recent victims of laptop security breaches include organisations in the retail, banking, public sector and local government markets. One local council had an employee laptop, containing the personal details of staff and former personnel, stolen during a street robbery. The council subsequently notified all affected staff and set up a hotline offering advice on how to protect themselves from potential identify theft.

Security breaches resulting from lost or stolen laptops can result in serious penalties, including heavy fines or permanent bans from obtaining and holding customer details in the future. This demonstrates the severity of such laxity in the eyes of regulatory bodies. Ineffective security policy enforcement can have a detrimental impact not only on the organisation but also on public confidence in personal data protection and the individuals' rights to privacy.

The threat of laptop breaches is even greater considering the startling number of management executives that are still unaware of the responsibility they have towards the protection of information held on them under the Data Protection Act (1998). In a rapidly changing, competitive, IT-driven environment, these executives have a growing cause to begin addressing security as a critical business issue on their agenda.

This concern is supported by the Information Commissioner's Office (IC), which calls for CEOs to take security of peoples' personal information more seriously and demands that privacy be given more priority in every UK boardroom.

One specific security issue that executives should be taking more seriously is laptop screen privacy and the omnipresent shoulder surfing threat. Today 65 per cent of UK businesses do not offer a comprehensive security policy that combats the issues of shoulder surfing. Key executives appear worryingly content to review confidential sales and personnel records on a laptop in a public place, leaving them at the mercy of complete strangers in the next seat or the row behind.

According to research commissioned by 3M, the diversified technology company, almost half of management professionals questioned (55 per cent) admitted to working on a laptop while on public transport and in shared work places at least once a week. 70 per cent of these workers also admitted to having personally experienced shoulder surfing. In

comparison to the public sector employees who are not so aware of their surroundings (51 per cent).

Surprisingly, this awareness of the potential risk has no correlation with the need for privacy as only 18 per cent of management professionals feel they need keep official documents private. However, they are making themselves understood that 'shoulder surfing' is not acceptable. 70 per cent of management executives claimed it caused some degree of discomfort and impeded work.

On the opposite side of the laptop, 80 percent of managers surveyed had admitted to shoulder surfing their neighbours when in public places. Reasons why laptops prove so attractive to inquisitive shoulder surfers is the promise of seeing business mail and corporate documents (34 per cent), posing a genuine threat to businesses wanting to protect sensitive information from falling into the wrong hands. Boredom (45 per cent), trying to get the lowdown on gossip (38 per cent) and scanning websites (14 per cent), were also popular triggers.

To protect laptop screens from unauthorised viewing and to help achieve data protection compliance, organisations can specify that all employees from the board down install a privacy filter device. Fitting neatly over any laptop or computer screen, privacy filters are designed specifically to allow an unrestricted view for the user but prevents others positioned to the side or viewing over their shoulder from seeing what is on the screen. The filters can also be readily removed and stored when not required. With the number of worldwide hotspots growing year on year, this level of privacy can give a greater sense of comfort to business travelers working in wi-fi friendly airports, hotel lobbies, coffee shops and other public places.

- Ends -

Contact information:

Tel: + 44 (0) 1344 858 576

Email: nhughes1@mmm.com

Web: www.3M.co.uk/privacyfilters

q0735mmm