

Protecting against laptop software theft

IDC research shows that 92% of SMEs with mobile workers have experienced laptop theft and 54% of SMEs have experienced a laptop theft in the past six months. "The laptop itself is not the issue, but the disruption to business and the risk to customer information, employee records or sensitive company data is far worse," warns J2 Software MD John McLoughlin.

Laptop theft occurs in a wide range of places, with public transport and hotels being particularly susceptible. The workplace is not immune from theft either, with 26% of IT managers suspecting internal involvement in the theft of laptops and just 35% of office-based theft being the result of a break in. Walk-in theft is almost as likely according to 31% of IT managers.

Laptop lockdown

McLoughlin says the laptop security market has a wide choice of products, from the tried and tested cable locks through to innovative Internet tracking services. "However, this does not solve the real issue at hand - data theft. The company has introduced a solution that protects computers and laptops from unauthorised access and offers free global theft cover."

The T3 SecurityKey is a security device that ensures instant lockdown, data encryption and covers one against theft, anywhere in the world. It ensures that unauthorised users cannot access one's PC or laptop to view, copy or modify confidential information. With passwords not being a real deterrent, this simple solution adds another layer of protection to keep the unwanted users at bay.

Insider information theft

Most companies do not have the tools to monitor users on the network but it is critical that access to information is managed and that users are held accountable for their actions. In addition, these systems should be unobtrusive and not interfere in daily tasks.

"Companies should be aware that employees are increasingly stealing confidential data and selling it for self gain, through removable media devices such as cellular phones, USB flash drives, removable hard disks, PDAs and MP3 players. Many organisations want simple tools to protect the network against security risks and data theft, but they don't realise what is happening with their information outside the building," he explains.

"Very little consideration has been given to providing solid management systems to ensure that the investment in technology delivers maximum benefit. It is extremely important that executives take corrective steps and ensure there are preventative measures in place. Organisations need to find comprehensive, simple-to-use solutions - based on a whole new set of emerging challenges and threats."

SystemSkan is designed to be a total user management tool that provides managers with the ability to view and record every user's actions on the computer network, including Internet and outgoing email attachments. It is used to identify security risks within an organisation, and provides policy enforcement tools to minimise these risks.

"SystemSkan will track, monitor and control every user activity on the network. It gives you visibility of what is really going across your network. It is an essential policy enforcement tool to manage networks, knowledge workers and to protect intellectual property. Our clients are enjoying massive savings, lowering their risk, increasing IT governance, aiding compliance and cutting bandwidth usage," he concludes.