

## HOW TO ENSURE SECURE REMOTE WORKING

By Ian Kilpatrick, chairman Wick Hill Group.

Businesses have never been under more pressure to reduce costs and operate efficiently, yet at the same time workers are increasingly demanding remote access to company applications and data.

There has been a rapid growth in the number of users requiring access - road warriors, employees working from home, day extenders, third parties such as contractors and partners, etc. In addition, both remote and office workers want the freedom to access from the office, from home or from a cybercafé.

These developments have accelerated the need for companies to provide users with secure access to their corporate desktop from any computer. However, there are major security implications in this scenario, made more serious by the increasing likelihood of financial repercussions for data breaches from organisations such as the Information Commissioner's Office (ICO) or the Payment Card Industry (PCI).

All this has created a headache for information security professionals, who have the unenviable task of managing and policing remote users with company laptops and home PCs. IT staff have to deal with user problems through the helpdesk, making sure that the anti-virus on their machines is up-to-date, and ensuring that all other updates and patches are installed. This is an expensive process and carries a number of security risks.

One approach to this problematic situation has been developed by leading security company Check Point. The company has come up with a product called Abra, a USB flash drive which serves as a plug-and-play secure, virtual office which can be used on any PC or laptop.

Abra creates a workspace where the user can access corporate files and applications securely. The user's session and the host PC are segregated, so users can even operate on what might normally be considered insecure machines. Built-in encryption protects data when working or travelling, ensuring PCI and ICO compliance.

The Abra type approach provides remote or roaming workers with considerable operational freedom, but they are still subject to the company's security policies. Indeed, for many companies, this approach can provide greater security management than existing arrangements.

The transfer of files between the PC hosting the Abra, and the corporate network, is strictly controlled. The use of applications and programmes too is subject to the applied security policy.

Only pre-approved applications are allowed to run within the secure virtual workspace. This effectively blocks the installation of malware and other threats. Abra can also block attempts to print from applications running inside this protected environment.

Security is enhanced by minimum password strength enforcement, as well as certificates and tokens for multi-factor authentication. A 'virtual keyboard' can be used at login to block password theft by key-loggers.

While Abra may not be the solution for all user environments, it is an ideal solution for organisations looking to let users purchase and manage their own PCs and laptops, and for those needing high security (including encryption) for devices outside the workplace

ENDS

June 2010

#### Bio of author

Ian Kilpatrick is chairman of value added distributor Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years. Wick Hill is an international organisation supplying SMEs and most of the Times Top 1000 companies through a value-added network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are the key factors in IT, rather than just technology. He has authored numerous articles and publications, as well as being a regular speaker at conferences, exhibitions and seminars.

For further press information, please contact Annabelle Brown on 01326 212130, email [abpublicrelations@btinternet.com](mailto:abpublicrelations@btinternet.com). For reader queries, please contact Wick Hill on 01483 227600, web [www.wickhill.com](http://www.wickhill.com).