

FEATURE

DON'T BE A LAPTOP LOSER

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure infrastructure solutions

Recently, a laptop containing salary details, addresses, dates of birth, national insurance numbers and phone numbers of some 26,000 employees went missing from a printing firm, which was writing to M&S workers about pension changes. Identity theft is the possible result of such losses. Also, at Worcestershire County Council, sensitive information about more than 16,000 council workers was put at risk as the result of another laptop theft.

At 28 police forces around the country, the instance of laptop thefts increased on average by 6% in 2006, with the Metropolitan police being the worst area for thefts with some 6576 laptops stolen. Devon and Cornwall area had a 45% increase in laptop thefts, rising from 276 to 401; and Bedfordshire saw a 35% increase. These figures only includes those laptops stolen while being used outside the office or home. And, of course, it ignores the large numbers lost in taxis, trains, buses, etc.

Awareness of the necessity to protect data resident on laptops is still very low in this country. According to the Department of Trade and Industry (DTI) Information Security Breaches Survey 2006, only one company in seven actually encrypts data on hard disks. The tendency is to be concerned with the cost of losing the machine rather than the cost of losing the data on it, which is likely to be a much higher expense.

Low awareness in the UK of these issues may be because we don't hear a lot about laptop losses. We just tend to hear about major faux pas, such as losses by the police, the military or government bodies.

UK companies and organisations are not actually compelled by law to inform users and public authorities if they lose sensitive data, and are naturally reticent to publicise their problems. However, they are still responsible for safeguarding personal information held on their systems under data protection laws and many other regulatory requirements.

If personal information is lost on a stolen laptop, there could be serious consequences for those to whom that information refers. Identity theft is one very worrying possibility. In addition to this concern, company sensitive information is often held on laptops, which businesses wouldn't want competitors or even anyone outside their organisation to see.

The irony of this situation is that companies can easily and inexpensively protect themselves from this kind of data leakage from laptops by using encryption software.

In the past, poor performance and high costs prevented the use of this type of solution, but today's high performance and low cost products make it impossible to justify not encrypting laptops. Such products can operate transparently in the background, so laptop users won't find them difficult to use.

Low-cost solutions are available, from companies such as Utimaco, which stop anyone who steals a laptop from deciphering what is on it. Utimaco's solution, for example, provides complete encryption of a laptop's hard disk, as well as a user authentication procedure which makes the hard disk secure.

Increasingly, as companies become more aware of high profile data losses through greater visibility, they are identifying areas where they need to deploy encryption - obviously on laptops, but also for e-mail, network attached storage, USBs, mobile devices, etc. This has lead to increased interest in UEM (Unified Encryption Management) solutions, which centrally manage encryption across an organisation and facilitate migration, over time, to a unified, organisation-wide encryption structure.

With the ever-increasing use of laptops out of the office, their vulnerability to theft and loss, and the availability of low-cost encryption solutions, now is the time for organisations to take the leap to securing laptops and avoid being laptop losers. By doing so, they protect their employees', customers' and partners' data from potential exposure, they meet their regulatory obligations, they avoid the wrath of shareholders, and they could be saving themselves an awful lot of money!

Most organisations experiencing a high profile data loss also add the cost of purchasing an encryption solution onto the high cost of dealing with the loss. If your company would do the same, then ask yourself if there could be any better ROI than choosing an encryption solution up front and preventing the problem in the first place!

ENDS

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, specialists in secure infrastructure solutions for ebusiness. Kilpatrick has been involved with the Group for 30 years and is the moving force behind its dynamic growth. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a 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 key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.