

February 3, 2009 Michael Herman

## Employees facing redundancy are tempted by data theft

A memory stick can contain vast amounts of data and is easily concealed

Companies face a new challenge in protecting sensitive information, says Michael Herman /A memory stick can contain vast amounts of data and is easily concealed.

However bad the economy gets and no matter how nervous white-collar workers become about losing their jobs, most are unlikely to sneak out of the office with a hard drive concealed under their jackets.

But when it comes to pilfering the contents of their office computers, many are far less scrupulous, leaving businesses with an enormous commercial and legal headache.

A recent survey from Cyber-Ark, the IT security group, found that 58 per cent of British workers would be prepared to take confidential company data if faced with redundancy. Perhaps more alarmingly, the same survey found that with job losses rising, 40 per cent of UK staff are already removing confidential data and would be willing to use it to help to negotiate a new job.



Cyber-Ark listed client or customer databases as the most likely forms of data to be stolen, followed by business proposals and product information. The financial services sector is traditionally considered the most at risk from employee data theft, but Mark Weston, a partner at Matthew Arnold & Baldwin, the law firm, said that it was a serious issue that affected all industries. Mr Weston argues that although criminal gangs are active in data theft, the single biggest threat is from a company's own employees, a point emphasised by a recent survey by McAfee, the IT security group, which found that 68 per cent of businesses were most concerned about the "insider threat".

The opportunities for removing data discreetly have improved in recent years through the availability of memory sticks. These are small devices - often the size of a pack of chewing gum - that can store many gigabytes of data and work with most office computers.

Adam Bosnian, a vice-president of Cyber-Ark, said: "The damage that insiders can do should not be underestimated. It can take just a few minutes for a database that has taken years to build to be copied to a memory stick. With a faltering economy resulting in increased job cuts, deferred promotions and additional stress, companies need to be especially vigilant about protecting data loss from nervous or disgruntled employees."

While some data can harm a business as soon as it is taken, much stolen information becomes a threat only once it is used by a competitor. So while the Cyber-Ark research found that well over half of British employees would be prepared to steal and use confidential data if faced with losing their jobs, it is perhaps

more alarming that statistics from the High Court show that British workers are increasingly making good on those intentions.

The number of court cases brought to stop former employees using confidential data in their new jobs climbed sevenfold between 2006 and 2008, according to Reynolds Porter Chamberlain (RPC), a law firm. The number of cases may have increased only from three to twenty-three, but RPC says that there will have been many more similar cases that were settled privately.

Cath Thorpe, an employment partner at RPC, said that the shaky economy and poor job prospects were directly to blame. “Rising job insecurity is encouraging more employees to use confidential information obtained from their current employer when they begin working for a competitor,” she said. Ms Thorpe added that with alternative jobs increasingly difficult to find, other employees are starting up their own businesses and “using confidential information in order to compete head-to-head with their former employer”.

Although litigation is expensive and not guaranteed, the 23 court cases brought last year should reassure business that it does have the ability to remove or reduce problems arising from employees jumping ship with confidential information.

In one recent high-profile case, UBS, the Swiss bank, sued Vestra, a start-up business formed by 78 former employees. The case settled on confidential terms, but not before a High Court judge gave an interim ruling barring Vestra from approaching any UBS clients.

Fast-moving employers have a more adventurous option, in the form of a “search and seize” order. Businesses with strong evidence of a former employee removing significant information - such as CCTV footage of someone leaving a secure data area with files - can apply for a court order authorising them to search the home of a former employee and remove company data.

Although the police are not involved, the former worker who obstructed the search would be in contempt of court, a criminal offence. Mr Weston warned that aside from having to get up early to catch them unaware, another downside to raiding the home of a former worker was that if nothing were found they may be able to claim compensation for the inconvenience.

Articles from our sister site:



Copyright 2010 Times Newspapers Ltd.

This service is provided on Times Newspapers' [standard Terms and Conditions](#). Please read our [Privacy Policy](#). To inquire about a licence to reproduce material from Times Online, The Times or The Sunday Times, click [here](#). This website is published by a member of the News International Group. News International Limited, 1 Virginia St, London E98 1XY, is the holding company for the News International group and is registered in England No 81701. VAT number GB 243 8054 69.