

Security worst case scenario: confidential data available at a car boot sale

- **Despite numerous warnings, much sensitive data is stored unencrypted on storage media and Notebooks**

Oberursel, April 6th, 2005 - Notebooks with secret government information which simply go missing, hard disks with sensitive company information which end up undeleted at car boot sales – claims for confidential information which has found its way into the public sphere unencrypted and inadvertently are heard month after month. This week an eBay user was able to purchase by auction a hard disk with internal alarm plans and name lists from a crisis management group. The Brandenburg Ministry of the Interior concerned is still puzzling over how it could have happened, since it normally has the data on its hard disk deleted by a security firm.

At the beginning of March, a pilferer took a Notebook with him from the administration office of a Californian university. In no time at all, he had not just the useful hardware, but the identity data for around 100,000 patrons, alumni and students including welfare security numbers and other sensitive information. Those concerned are still afraid the thief may use the data for his own purposes.

In the USA, a twenty-one year old hacker helped himself to the server of a national telecommunications provider. He found secret documents from the CIA. And 1.2 million participants of the American government's Smartpay programme were worried that their accounts might have been emptied. Back up tapes were completely lost on their way to the data processing centre. The speaker for the bank responsible expressed "deep regret".

Cases like these show that data theft or data loss is not just embarrassing, but expensive, damaging to business and, in the most serious cases, can be ruinous for a company. The solution, which applied would have prevented the problems in the first place, is however very simple: encryption of all important data. The leading supplier of software solutions in this field is Utimaco. Its product SafeGuard Easy transparently encrypts the entire contents of the hard disk. This means that the user– if the programme is installed only once - doesn't need to worry any longer about encrypting his or her data, because this takes place automatically in the background. The finder – or thief – of a Notebook protected in this way will see only scrambled data when files are opened. The same can be implemented for PDAs or Smartphones whilst simultaneously increasing the obstacles to access for unauthorised persons.

"If, alongside secure user authentication, encryption of data is also guaranteed a Notebook is secure in combination with the classic preventative measures such as virus protection" says Ansgar Heinen, security expert at Utimaco. "That applies to private users too, who have holiday photos and personal data saved on their Notebooks. The virtual assets which can be lost from a Notebook are often just as important for this user as the sensitive and valuable customer, product or company information stored on a company's Notebook.

Should a well-protected laptop fall into the wrong hands through negligence or theft, at least the data remains forever unreadable. Although the PC has been lost, the damage is limited.

Further information about solutions for secure mobile working and Utimaco are available at <http://www.utimaco.com>

Utimaco Safeware AG is one of the leading technology manufacturers of professional solutions for IT security. The security technologies and solutions developed by Utimaco Safeware protect electronic values of companies and authorities from unauthorized access and guarantee that business processes and administration procedures are binding and confidential.

The business unit Personal Device Security provides technologies and solutions to guarantee mobile security in the fields of strong authentication, including biometric procedures, encryption and integrity control. The products and solutions secure data in Terminal Server and Citrix environments, on PCs, Laptops and PDAs.