Software watching while you work

Software that can not only monitor every keystroke and action performed at a PC but also be used as legally binding evidence of wrong-doing has been unveiled.

Worries about cyber-crime and sabotage have prompted many employers to consider monitoring employees. The developers behind the system claim it is a break-through in the way data is monitored and stored. But privacy advocates are concerned by the invasive nature of such software.

The system is a joint venture between security firm 3ami and storage specialists BridgeHead Software. They have joined forces to create a system which can monitor computer activity, store it and retrieve disputed files within minutes. More and more firms are finding themselves in deep water as a result of data misuse. Sabotage and data theft are most commonly committed from within an organisation according to the National Hi-Tech Crime Unit (NHTCU) A survey conducted on its behalf by NOP found evidence that more than 80% of medium and large companies have been victims of some form of cyber-crime. BridgeHead Software has come up with techniques to prove, to a legal standard, that any stored file on a PC has not been tampered with. Ironically the impetus for developing the system came as a result of the Freedom of Information Act, which requires companies to store all data for a certain amount of time.

The storage system has been incorporated into an application developed by security firm 3ami which allows every action on a computer to be logged. Potentially it could help employers to follow the trail of stolen files and pinpoint whether they had been emailed to a third party, copied, printed, deleted or saved to CD, floppy disk, memory stick or flash card. Other activities the system can monitor include the downloading of pornography, the use of racist or bullying language or the copying of applications for personal use. Increasingly organisations that handle sensitive data, such

as governments, are using biometric log-ins such as fingerprinting to provide conclusive proof of who was using a particular machine at any given time. Privacy advocates are concerned that monitoring at work is not only damaging to employee's privacy but also to the relationship between employers and their staff. "That is not the case," said Tim Ellsmore, managing director of 3ami. "It is not about replacing dialogue but there are issues that you can talk through but you still need proof," he said. "People need to recognise that you are using a PC as a representative of a company and that employers have a legal requirement to store data," he added.