Staff no longer able to get away with crime at their PCs: new software monitors and records their every action

Submitted by: Omarketing Limited
Wednesday, 19 January 2005

FOR IMMEDIATE RELEASE
PR04/BHS/NAT
www.BridgeHeadSoftware.com
19th January 2005

Pesky staff to get away with it no longer: we were watching you and we can prove it, too

‘Compliance-standard’ proof of wrongdoing to deter employees-turned-saboteurs

Ashtead, UK – 19th January 2005 - With cyber-crime on the increase and all-too-often “an inside job”, two UK technology companies have collaborated to develop a way for companies not only to find out “whodunit” - but to prove it more easily in court, too.

IT security specialist 3ami and storage specialist BridgeHead Software have unveiled a radical piece of software that monitors and records every keystroke and every action performed at any PC in an organization – and that can subsequently provide legally-admissible proof of the wrong-doing or other unapproved activity.

While such software typically provokes cries of “Big Brother!”, the facts support its use. In 2003, NOP research for the National Hi-Tech Crime Unit (NHTCU) suggested that more than 80% of medium and large companies experienced hi-tech crime in 2003.

Significantly, acts of sabotage (at 53%) and data theft (56%) were most often committed from within an organization. Also, more than a third of incidences of financial fraud were either wholly, or partially, perpetrated by employees.

The difficulty to date for companies has been in identifying the perpetrator, and in subsequently proving what happened in a court of law. However, increasing use of sophisticated authentication techniques such as fingerprint scanners instead of passwords has made finding out the ‘who’ considerably simpler.

Now – ironically as an indirect result of Government compliance and regulatory initiatives that followed the recent Enron and WorldCom scandals, and the Freedom of Information Act – proving the ‘what’ has also been made possible.

The breakthrough in this case has been made by storage specialist BridgeHead Software. To help companies meet so-called compliance regulations, BridgeHead has developed techniques that can prove, to a legal standard, that any file, once stored, has not been tampered with, i.e. altered, moved or copied. This technology has been adopted by security specialist 3ami and incorporated into its own Monitoring, Audit & Security (MAS) application.

As 3ami’s MAS logs every keystroke and action on a computer, BridgeHead’s technology records it in a

tamperproof data file. This enables management to identify and later to prove all instances of:
- theft of data files, including by emailing to a third party, by copying, printing or deleting, by saving to CD, floppy disk, USB memory stick or flash card
- upload or download of confidential files, pornography or other illegal images
- use of racist, libelous, sexist, discriminatory, bullying or abusive language
- theft by copying applications for personal use

The result is a system that, while it does not actually prevent acts of sabotage, theft, fraud or system damage, does at least offer organizations a means to respond. And, by informing all staff in advance of the prospect of detection and prosecution, in theory at least many would-be saboteurs will be deterred from their course of action.

Tony Cotterill, CEO at BridgeHead Software, said: “In a medium or large company environment, where there are computer experts, someone charged with wrongdoing might once have successfully argued that some unknown third party had forged their activity log to make it look like they were acting illegally. Now that’s not going to be a valid defense because BridgeHead can prove the veracity of a file. It’s a great asset for business managers, who can now answer the question: how can I know for sure what my staff members are doing at their computers?”

Tim Ellsmore, Managing Director of 3ami, said: “Firewalls and virus protection will only get a company so far – about halfway there, according to the research. Now, we can prove that what MAS recorded is what really happened – and knowing that you’re going to get caught has got to be a strong deterrent to wrongdoing.”
[ends]

Notes to editors
BridgeHead’s intelligent storage management technology ensures true data is economically stored, and that all access and movement of that data is audited; through the use of policies, data can also be set to be deleted at the stipulated ‘end-of-life’. With all files in secondary storage fully secured, but accessible and indexed, data can be searched and information retrieved, and it can be proved that the data has not been tampered with or altered.

Press contacts
Rose Ross and Hannah Knowles
Omarketing Limited (for BridgeHead Software)
T: +44(0) 20 8255 5225
E: Rose@omarketing.co.uk / Hannah@omarketing.co.uk

About 3ami (www.3ami.com)
3ami is a systems integration business with a particular specialisation in securing both electronic infrastructure and the data that resides on it. It constantly monitors security threats and identifies technologies to protect businesses from such threats, scouring the market to identify the most effective and cost efficient solutions.

3ami meets the needs of businesses ranging from SMEs requiring a few additional anti-virus software

licenses, to large organisations needing an EAL4+ certified firewall, installed by security-cleared engineers. 3ami is based in Manchester, UK.

About BridgeHead (www.BridgeHeadSoftware.com)
BridgeHead is a technology company with a total focus on storage management software. Over the past 10 years, BridgeHead has supplied its technology to large application and hardware vendors like Dell, MEDITECH, EMC, HP, and IBM, to facilitate their customers' storage management needs.
Founded in 1994, with corporate offices in the UK, USA, and Germany, BridgeHead Software's multi-platform software solutions are designed for Archive, enterprise backup, media management and disaster recovery.

NOTE: All trademarks and registered trademarks are the properties of their respective owners.