

### PRESS CONTACTS:

#### Strategic Alliance International

Amy Redhead  
amy@strategicpr.net  
01494 434 434

#### Network Instruments

Vanessa Wauters  
vanessaw@networkinstruments.co.uk  
+ 44 1959 569 880

### Organisations Lack Ability to Investigate Compliance Violations and Network Security Breaches

#### Half of Organisations Doubt Ability to Ensure Compliance

*London, UK – 21 August 2007* – New regulations increasingly require organisations to monitor and document network activities to ensure compliance. Nevertheless, a recent survey by Network Instruments, a provider of network monitoring and analysis solutions, found that only 16 per cent of network professionals feel confident their current network tools are efficient enough to validate and support data compliance with government regulations.

In the survey involving over 125 industry professionals including CIOs, engineers, and IT managers from Europe and North America, 40 per cent of respondents indicated a need to improve their ability to track network security breaches.

In coming years, security and compliance will become an increasing burden on IT departments with government regulatory acts such as Sarbanes Oxley (SOX), HIPAA, BASEL II forcing companies throughout the world to actively investigate and document any violation that occurs on the network.

“Undoubtedly, compliance has a great impact on the entire IT infrastructure,” said Ian Cummins, European sales director for Network Instruments. “Effective retrospective analysis, monitoring and troubleshooting tools can help support IT’s role in compliance by providing a mechanism for monitoring and documenting financial and other activity on the network, streamlining the enforcement process and providing network managers with the ability to validate and provide evidence for compliance and security issues.”

Corporate network users are one of the most common causes of compliance breaches. Breaches can include disabling a security client, introducing malware into the network or even leaving a workstation unlocked when the user is away from their desk. 30 per cent of respondents expressed an inability to enforce internal HR policies, indicating many organisations may not have the tools required to monitor and report on unauthorised network and internet behaviour and ensure that corporate network policies are met.

Retrospective network analysis tools, such as Network Instruments’ GigaStor™, provide continuous packet captures containing days, weeks, or months worth of network data. They can then sift quickly through the massive amounts of traffic to find the specific policy violation or anomalous traffic causing any network degradation, eliminating the need to recreate the problem. This ability to carry out historical analysis and reconstruct data streams is extremely valuable not only for monitoring and detecting whether a security breach or access violation has taken place but also for demonstrating compliance management to auditors.

###

#### About Network Instruments

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments’ Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimises network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner and NI University please visit [www.networkinstruments.co.uk](http://www.networkinstruments.co.uk).