**New Best Practice Guide from CCSS Identifies Security Threats to IBM System i Environments**

***January 14, 2011* – CCSS,** the leading systems management solution developer for IBM System i and Power Systems platforms, has issued a new guide in their 'Best Practice' series to help system managers identify and resolve some of the most damaging and difficult to detect security issues that can occur in even the most robust and carefully managed environments. The guide covers security issues that represent some of the most serious and elusive threats to system availability, data integrity and user productivity levels, all of which can have damning financial consequences for the company concerned if they remain unmonitored.

The guide examines the multi-layered nature of security breaches on the system i and looks at how primary problems are often masked by secondary issues which require immediate attention. An example of this is given to illustrate how an instance of high CPU can slow down the machines and impact the user community. In this case, additional processors on demand could stem the fallout, but this would be a costly and temporary approach which did little to address the root cause – a looping authority failure which generated thousands of entries. The duel task for IT Managers and system administrators facing this type of scenario is first to identify the root cause and then to resolve it quickly. The latter job of investigation is also a critical factor in reducing the associated costs of any security threat to the system.

In the example of the looping authority failure above, real-time monitoring of the security audit journal could have isolated the root cause immediately and minimized any impact on the user community. A process of real-time conversion of journal entries to messages allows these types of problems to be escalated to the immediate attention of managers. Swift action to identify the file in the IFS can then be taken and once authority is granted, CPU levels can return to normal levels with no requirement for lengthy investigative procedures or the purchase of additional resource.

Paul Ratchford, Product Manager for CCSS, explains how the new guide can help to eliminate risk 'hot spots' in a System i environment, "When we talk about security issues, it's not just a malicious threat from the outside, it also includes situations that breach internal protocols that are not driven by any sort of sinister motivation and also, the circumstances that can leave the system vulnerable to attack, whether one occurs or not. The guide aims to assess these common areas of risk exposure and offers solutions to eliminate them with real-time Security Audit Journal monitoring, FTP monitoring and network monitoring."

CCSS suggests the most effective solution to eliminating security risks in any System i environment is to tackle the problem from the inside out. This can be done by adapting systems management protocols to embrace security issues and thereby reducing their potential for harm. A pro-active approach targets both the primary issue, i.e. the breach itself, and in doing so, wards off the occurrence of any negative secondary issues, such as poor system performance or the need for knee-jerk spend initiatives as temporary solutions. In this way, IT Managers who might otherwise be wrestling with the multiple negative consequences of security issues have an opportunity to embrace the multiple benefits of this pro-active approach instead. The rewards for doing so not only maximize the productivity of a busy user community but extend to meeting regulatory and audit compliance issues, reducing unexpected resource expenditure and reducing the intensive burden of investigation for time-strapped IT Managers.

To download the guide in full, please visit:
http://www.ccssltd.com/resources/best-practice.php

Or join the CCSS Linked In Group:
http://www.linkedin.com/groups?mostPopular=&gid=1771585

For more information on CCSS, Security Audit Journal Monitoring and QMessage Monitor, please visit:
http://www.ccssltd.com/products/qmessage-monitor/

**ENDS**

**About CCSS**

CCSS develops, supports and markets IBM i (on Power Systems & System i servers) performance monitoring and reporting, message management and remote management solutions. An Advanced IBM Business Partner, CCSS develops powerful solutions to support some of the world's most demanding IBM i environments across many industries including insurance, banking, pharmaceutical and manufacturing. Existing customers that rely on CCSS's feature-rich solutions include leading organizations such as Volvo, Mattel, Newell-Rubbermaid, The Royal Bank of Scotland, and Siemens Healthcare.

CCSS is headquartered in Gillingham, Kent, UK with key regional headquarters in Raleigh, North Carolina, USA and Bonn, Germany together with a global agent network spanning Austria, Portugal, the Netherlands, Switzerland and Sweden.

**www.ccssltd.com**